UNIVERSIDAD DE CUENCA

Facultad de Ingeniería

Carrera de Electrónica y Telecomunicaciones

Desarrollo de una solución para la extracción de evidencia forense sobre la actividad de un usuario de un dispositivo móvil

Trabajo de titulación previo a la obtención del título de Ingeniera en Electrónica y Telecomunicaciones.

Autora :
Jessica Paola Camacho Cajamarca C.I. 0301836466
Directora :
Ing. Karina Pamela Campos Argudo, Mgst C.I. 0103143830
Co-Directora :
Ing. Irene Priscila Cedillo Orellana, PhD C.I. 0102815842

Cuenca - Ecuador

2018

Resumen

Hoy en día los dispositivos móviles han evolucionado vertiginosamente debido a su adopción masiva por parte de los usuarios, que incluso llegan a tener varios dispositivos con diferentes propósitos. Estos dispositivos contienen una mayor capacidad / funcionalidad para administrar la información, con las características integradas que se convierten en un importante contenedor de evidencia digital. En los últimos años, se han llevado a cabo investigaciones considerables sobre diversas pruebas electrónicas digitales, esquemas de adquisición y métodos para extraer evidencia de dispositivos móviles. La investigación debe seguir protocolos basados en estándares nacionales como internacionales y considerar recomendaciones para el correcto manejo de la evidencia.

El objetivo principal del trabajo de titulación es plantear un proceso para el Análisis Forense Digital en dispositivos móviles, proporcionar técnicas científicas y desarrollar una herramienta que proporcione un registro de actividades del usuario. A la vez, este documento contiene una prueba de concepto para demostrar su vialidad.

Palabras clave : Análisis forense, dispositivo móvil, Android, herramienta forense.

Abstract

Mobile devices have evolved vertiginously due to their massive adoption by users, who have several devices with different purposes. These devices contain greater capacity/functionality to manage information, with the embedded characteristics they become an important digital evidence container. In recent years, considerable research has been conducted on various digital electronic evidence, acquisition schemes and methods of extracting evidence from mobile devices. The research must follow protocols based on national and international standards and consider recommendations for the correct handling of the evidence.

The main objective in this work is to propose a process for Digital Forensic Analysis in mobile devices, provide scientific techniques and develop a tool that provides a record of user activities. At the same time, this document contains a case study to prove its viability.

Keywords : Analysis forensic, mobile device, Android, forensic tool.

Índice general

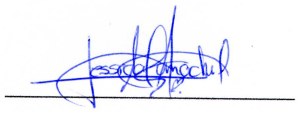
Índice de figuras

Índice de tablas

Cláusula de Propiedad Intelectual

Yo, Jessica Paola Camacho Cajamarca, autora del trabajo de titulación "Desarrollo de una solución para la extracción de evidencia forense sobre la actividad de un usuario de un dispositivo móvil", certifico que todas las ideas, opiniones y contenidos expuestos en la presente investigación son de exclusiva responsabilidad de su autora.

Cuenca, 19 de octubre de 2018



Jessica Paola Camacho Cajamarca

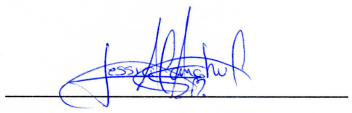
C.I: 0301836466

Cláusula de licencia y autorización para publicación en el Repositorio Institucional

Yo, Jessica Paola Camacho Cajamarca en calidad de autora y titular de los derechos morales y patrimoniales del trabajo de titulación "Desarrollo de una solución para la extracción de evidencia forense sobre la actividad de un usuario de un dispositivo móvil", de conformidad con el Art. 114 del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN reconozco a favor de la Universidad de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos.

Asimismo, autorizo a la Universidad de Cuenca para que realice la publicación de este trabajo de titulación en el repositorio institucional, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Cuenca, 19 de octubre de 2018



Jessica Paola Camacho Cajamarca

C.I: 0301836466

Dedicatoria

A mi madre María.

Por el ejemplo de mujer que fue, por sus consejos, valores y la motivación que me dio y que aún lo tengo presente, lo que me ha permitido ser una persona de bien, pero más que nada, por el amor que me brindó y que tanto extraño.

A mis abuelos.

Papio y Mamilola, quienes con su ejemplo de humildad, sencillez, trabajo duro y amor forjaron mi carácter.

¡Siempre estarán en mi corazón!

Jessica Camacho

Agradecimientos

Estas líneas de agradecimiento significan que ha llegado el final de mi etapa universitaria. En primer lugar me gustaría agradecer a mi familia, principalmente a mi padre y hermanos por el apoyo en todos estos años. A mis tíos Genaro, Hilda, Segundo, Anabel, Benjamín, Magdalena y a todos aquellos que siempre me apoyaron y creyeron en mi.

En segundo lugar me gustaría agradecer a Ismael, Estefanía, Cristihan y Andrés, que me han dado el ánimo que me faltaba durante esos últimos meses y sobre todo a Dario, por ser la persona que me apoyo durante mi carrera. También quiero hacer mención a los amigos y compañeros que he hecho durante estos años.

Finalmente agradezco a las Ingenieras Karina Campos y Priscila Cedillo por ofrecerse a dirigir este proyecto, tan distinto a lo que se suele ver normalmente en este tipo de estudios universitarios. Por su ayuda en el desarrollo del mismo y a quienes participaron directa o indirectamente en la elaboración de esta tesis.

¡Gracias a ustedes!

Jessica Camacho

Abreviaciones y Acrónimos

ACM Association for Computing Machinery. 28
ADB Android Debug Bridge. 22, 36, 79, 83, 135
AENOR Asociación Española de Normalización y Certificación. 17
API Interfaz de Programación de Aplicaciones. 12
AVD Android Virtual Devices. 37

BES BlackBerry Enterprise Server. 14
BIS BlackBerry Internet Service. 14

CdC Cadena de Custodia. 11, 46
COIP Código Orgánico Integral Penal. 3, 18, 47

DFF Digital Forensics Framework. 34
DFRWS Digital Forensics Research Workshop. 36
DVM Maquina Virtual Dalvik. 12

EXIF Exchangeable image file format. 21

FTK Forensic Toolkit. 36, 37

GPS Global Positioning System. 34

HDFI Harmonized Digital Forensics Investigation. 36

IEC International Electrotechnical Commission. 2, 11, 17–19, 44
IETF Internet Engineering Task Force. 17, 19
INEC Instituto Nacional de Estadística y Censo. 14, 15
iOS i Operative System. 12–14, 20, 36–38, 40, 95
ISO International Organization for Standardization. 2, 11, 17–19, 44
IUI Inteligents User Inferface. 26

JTAG Joint Test Action Group. 36

MIDP Mobile Information Device profile. 14

NIST National Institute of Standards and Technology. 44

OWASP Open Web Application Security Project. 21

PIM Project Management Institute. 162
PIN Personal Identification Number. 20, 50, 79, 131

RAM Random Access Memory. 21, 34, 75, 76, 83
RFC Request for Comments. 2, 18, 19, 44
RIM Research In Motion. 14
ROM Random Only Memory. 34

SGEE Sistema de Gestión de Evidencia Electrónica. 19
SGSI Sistema de Gestión de Seguridad de la Información. 19
SIM Subscriber Identity Module. 34, 75, 132
SLR Systematic Literature Review. 26
SO Sistema Operativo. 2, 9, 12–14, 16, 21, 22, 34, 40, 58, 62, 63, 68, 72, 95
SO-móvil Sistema Operativo móvil. 11, 12
SWGDE Scientific Working Group on Digital Evidence. 45

TI Tecnologías de la Información. 19
TSK The Sleuth Kit. 37

WAP Protocolo de Aplicaciones Inalámbricas. 14

Capítulo 1

Introducción

En este capítulo, se presenta por un lado en la sección 1.1 la motivación del problema así como la justificación y el alcance. La sección 1.2 muestra los objetivos general y específicos del trabajo. La sección 1.3 expone los pasos involucrados en la investigación y la sección 1.4 muestra como se desglosa el trabajo en siete capítulos incluido las conclusiones.

1.1. Motivación

Actualmente, los dispositivos móviles se han convertido en una herramienta de comunicación indispensable a nivel personal y laboral. Estos dispositivos están evolucionando de tal manera que no sólo se almacena información útil para el usuario (contactos, música y vídeo), sino que también pueden constituir una fuente de evidencia importante para un análisis forense que sirva de soporte para el esclarecimiento en ciertos casos judiciales [7]. Al existir una gran diversidad de fabricantes de dispositivos en el mercado cada uno con una distribución de Sistema Operativo (SO) y versiones distintas [7], se puede complicar el correcto manejo de cada uno de los dispositivos implicados por parte del examinador forense. Los SO basados en Android, se han posicionado como el actual líder del mercado, generando un desafío debido a la gran cantidad de versiones existentes. La siguiente empresa con mayor número de clientes es Apple con una menor penetración de mercado y de código cerrado, pero con menos versiones existentes [8].

Por otra parte, en el análisis forense converge un conjunto de técnicas que permiten recopilar y extraer información de distintos dispositivos sin alterar su estado original [9]. Por ejemplo, se pueden recuperar archivos borrados, historial de navegación, información de mensajería instantánea, datos de inicio de sesión, entre otros. A toda esta información se la conoce como evidencia digital. Sin embargo, en muchas ocasiones la información no es relevante, ésto hace que el investigador examine información poco práctica [10]. Según León [11] se deben tomar en cuenta tres aspectos para el análisis forense: i) evitar la contaminación de la evidencia para prevenir interpretaciones erróneas; ii) actuar metódicamente, es decir, todos los resultados del proceso forense deben ser bien documentados; y iii) controlar la cadena de custodia respondiendo a una diligencia y formalidad especial para documentar. En la investigación forense también existen aspectos legales que no siempre son cumplidos, ésto conlleva al uso indebido de aplicaciones, fraudes, robos, diseminación de materiales con derechos de autor, etc. El análisis realizado por Taylor et al., [12] indica que, para la obtención de evidencia digital, se deben seguir los lineamientos legales correspondientes a la jurisdicción en donde se genera el conflicto, ésto para evitar la exposición indebida de los datos personales. Por otro lado, de lo que se ha revisado hasta el momento, no existe ninguna herramienta en el mercado, que permita extraer una bitácora del comportamiento de un propietario para un dispositivo móvil.

El presente trabajo de titulación, busca generar un proceso y herramienta para que cumpla con: identificación, adquisición y análisis de evidencia recuperada desde dispositivos móviles con SO Android y versiones de prueba de ciertas aplicaciones para la extracción de información, que abarque la extracción de datos considerando las recomendaciones que proponen los estándares y normas internacionales tal como: i) ISO/IEC 27037 [13], este estándar proporciona directrices en el escenario de identificación, recolección, adquisición y preservación de la evidencia digital;

ii) RFC 3227 [14], proporciona de igual manera directrices para la recopilación y archivo de las pruebas; iii) UNE 71505 [15], proporciona buenas prácticas en la gestión de evidencia. Adicionalmente, se debe acoger a leyes nacionales vigentes como son: Código Orgánico Integral Penal (COIP) [16] y Ley de comercio electrónico, firmas electrónicas y mensajes de datos [17]. Además, se proporciona una herramienta que permite crear un registro de actividades sobre el uso de un dispositivo móvil, es decir, se trata de una herramienta de software que pretende automatizar el trabajo forense.

Debido a que la herramienta es exclusivamente para uso forense, la solución está orientada a peritos técnicos forenses, quienes estén actuando en el análisis de la evidencia que involucre un dispositivo móvil, proporcionado por los actores de un caso y bajo la autorización legal correspondiente. Los usuarios serán quienes deban acogerse a dos principales leyes: i) medio de prueba en donde se indica que todos los mensajes de datos, correos electrónicos, entre otros, servirán para efectos legales y ii) la valoración de la prueba la cual se someterá a criterio judicial a través de la evaluación realizada por un juez o un árbitro competente quien deberá designar al perito para el análisis y estudio tecnológico de las pruebas presentadas [17].

1.2. Objetivos

1.2.1. Objetivo General

Desarrollo de una herramienta y proceso que cuenten con las directrices necesarias para realizar un análisis forense de las actividades del usuario del dispositivo móvil.

1.2.2. Objetivos Específicos

- Realizar un estudio exhaustivo del estado actual de la investigación en cuanto a la recolección de evidencia digital y análisis forense en dispositivos móviles.
- Diseñar y desarrollar un proceso que permita el análisis, recopilación y extracción de evidencia digital generada por las actividades del usuario en el dispositivo móvil.
- Definir los parámetros necesarios que serán utilizados durante la aplicación del proceso forense.
- Desarrollar una herramienta que permita presentar la generación de un registro de actividades sobre el uso del dispositivo móvil en un tiempo determinado.
- Evaluar a través de pruebas de concepto y/o casos de estudio la viabilidad de esta propuesta.

1.3. Tareas de investigación

Las tareas de investigación del presente trabajo están basadas en el método cuantitativo de Hernández et al., [1], cabe destacar que esta metodología no debe confundirse con el proceso metodológico forense sino que èsta nos permitirá lograr un trabajo de investigación apegado al método científico. El método de investigación proporciona una serie de pasos que permiten obtener los resultados esperados como se observa en la Figura 1.1.

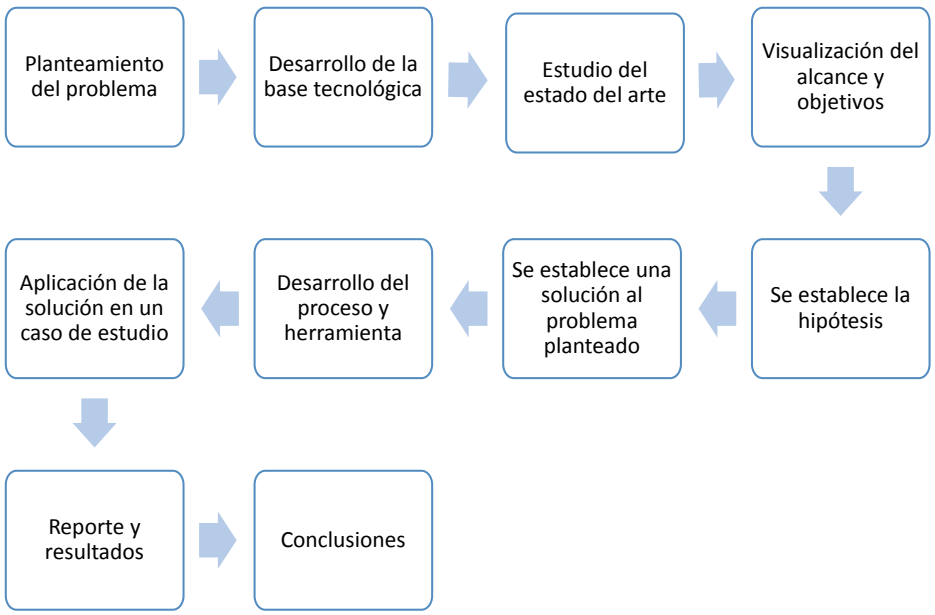


Figura 1.1: Tareas de investigación [1].

- **Planteamiento del problema:** Se realizará la delimitación del problema de estudio y el método que se va a utilizar para llevar a cabo una investigación apropiada.
- **Desarrollo de la base tecnológica:** Para la base tecnológica se recopila toda la información relacionada con el problema.
- **Estudio del estado del arte:** Se realiza un estudio de mapeo sistemático y permitirán tener un estado actual de la literatura.
- **Visualización del alcance y objetivos:** Se analizaron los resultados del estudio realiza-

do en el estado del arte para delimitar el alcance y los objetivos que tendrá la investigación.

- **Se establecer la hipótesis:** A continuación se halló que existe falta de estudios con respecto a las actividades que un usuario realizó en un dispositivo móvil.
- **Se establecer una solución al problema planteado:** Se desarrolló un proceso forense y una herramienta para extraer las actividades de un usuario en el dispositivo móvil.
- **Desarrollo del proceso y herramienta:** Se planifica la forma de elaborar el proceso para el análisis forense y el desarrollo de la herramienta.
- **Aplicación de la solución en un caso de estudio:** En este paso se pondrá en práctica el proceso y la herramienta analizando un teléfono celular.
- **Reporte y resultados:** Se detalla los resultados de la investigación forense en un informe técnico y ejecutivo
- **Conclusiones:** Se sacarán las conclusiones más relevantes del trabajo.

1.4. Estructura del trabajo

El siguiente trabajo está distribuido en siete capítulos de la siguiente manera:

- **Capítulo I: Introducción**
  Se da un enfoque general de los conceptos existentes, se define el problema y la justificación para el desarrollando del trabajo.
- **Capítulo II: Base Tecnológica**
  Se realiza una recopilación, definición y entendimiento de todos los términos asociados al análisis forense, dispositivos móviles y normas nacionales e internacionales, así como también se definen los conceptos claves y necesarios para el desarrollo y entendimiento del trabajo.
- **Capítulo III: Estado del Arte**
  Contiene el estado actual de la investigación por medio de una revisión sistemática de las temáticas propuestas.
- **Capítulo IV: Desarrollo del proceso para la investigación**
  Seguir un proceso metodológico es primordial para el éxito de una análisis forense digital. Se explica los diferentes pasos para el análisis en dispositivos móviles.
- **Capítulo V: Herramienta**
  Se desarrolla una herramienta que generará un documento con el registro de actividades que el usuario realizó en su dispositivo en un tiempo determinado.
- **Capítulo VI: Prueba de concepto**
  Mediante un caso impuesto se podrá comprobar el procesos y la herramienta que fueron desarrollados.
- **Capítulo VII: Conclusiones y Recomendaciones**

Finalmente, se desarrollan las conclusiones respectivas del trabajo, así como recomendaciones para trabajos futuros.

En la Figura 1.2, de autoría propia se muestra la estructura del trabajo a la vez que se cumplen las tareas de investigación realizadas.

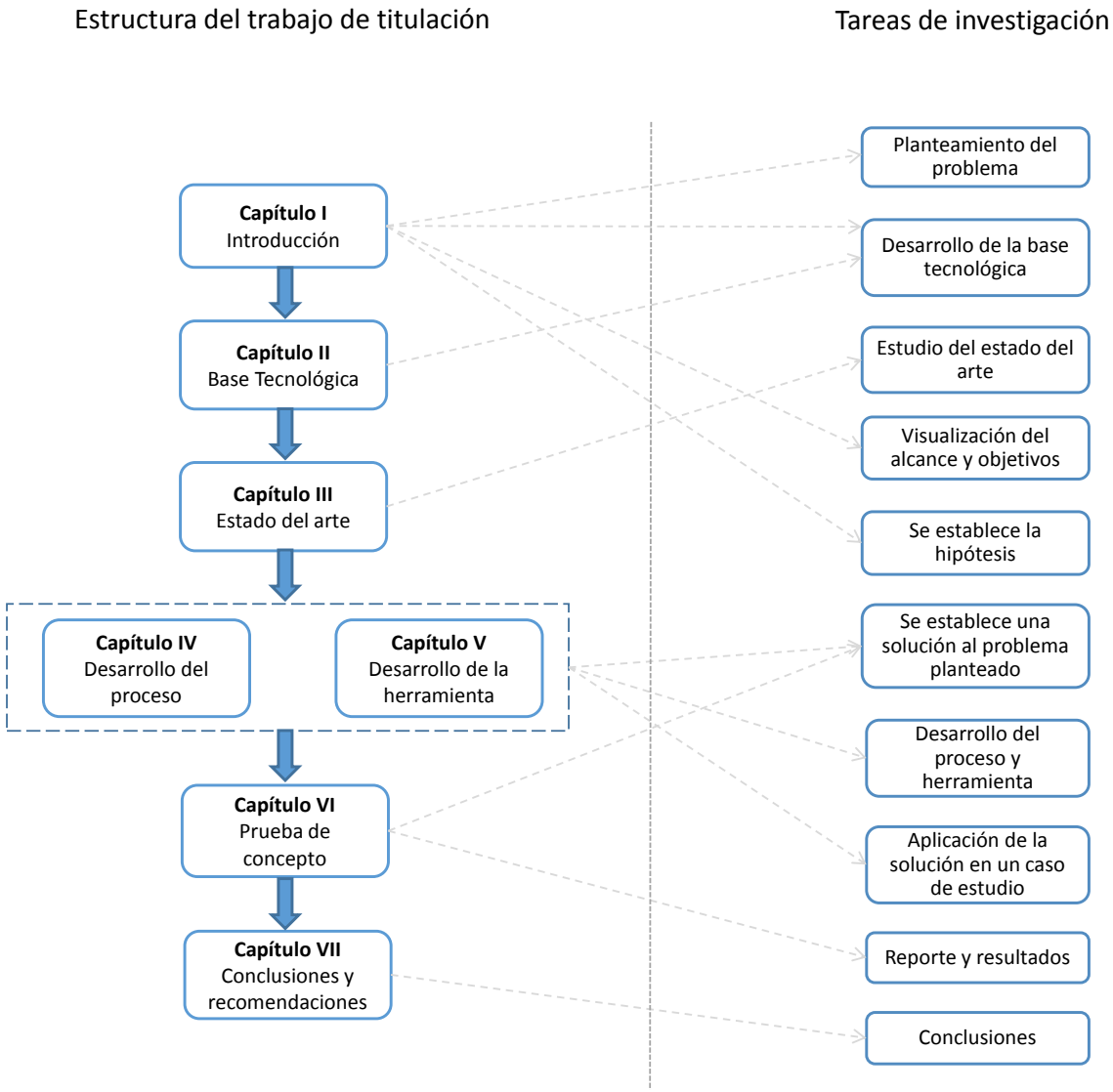


Figura 1.2: Estructura del trabajo.

Capítulo 2

Base Tecnológica

En este capítulo, se aborda todos los términos considerados importantes así como definiciones y teorías relacionadas con la informática forense y dispositivos móviles. En la sección 2.1 se da una breve introducción al capítulo, la sección 2.2 trata sobre términos generales de informática forense, la sección 2.3 da una explicación de los Sistemas Operativos (SOs) existentes y con mayor acogida, en la sección 2.4 se estudian los estándares, normas y regulaciones que se toman en cuenta en la investigación forense y finalmente, en la sección 2.5 se definen las herramientas que se van a utilizar en el trabajo.

2.1. Introducción

En este capítulo se presenta un análisis de los conceptos principales para lograr que el trabajo de titulación sea auto-contenido, para de esta manera situarse en el contexto y establecer bases para el desarrollo de trabajo. También se realiza una revisión a la regularización estatal en cuanto al marco jurídico, Código Penal y las leyes que se deben conocer para realizar un análisis forense. También se revisará las normas y estándares internacionales, que están relacionadas con el tema forense especialmente orientado a dispositivos móviles. Finalmente, se hace un repaso de las herramientas para la extracción de los datos necesarios para el desarrollo de la herramienta.

2.2. Informática forense

La informática forense es una ciencia que se encarga de asegurar, preservar, identificar, analizar y presentar un conjunto de datos. También se lo define como un conjunto de herramientas y técnicas que facilitan no solo el análisis, sino con finalidades de prevención [18].

2.2.1. Análisis forense digital

López [19] señala que, el análisis forense es una disciplina relativamente nueva y está orientada a la investigación de delitos. Según el mismo autor es un método científico que identifica, preserva, analiza y presenta los datos e información que proviene de dispositivos digitales.

Edmond Locard, es conocido por su famoso principio de Intercambio de Locard. El principio dice que cada vez que se hace contacto con otra persona, lugar o cosa, el resultado es un intercambio de material físico. Cuando ha ocurrido un delito informático, el investigador de la escena del crimen debe reconocer, documentar y recolectar evidencia y de algo o alguien que tenga contacto con la escena del crimen. Aunque no se da un intercambio físico entre dispositivos, este principio se puede aplicar al análisis forense digital ya que se realiza una transferencia de rastros lógicos [20].

Los dispositivos móviles también son objeto de investigación y análisis forense digital, la información que se puede identificar son: datos personales, historial de navegación, números telefónicos, agenda, multimedia, aplicaciones, mensajería, correos electrónicos, etc., debido a todas estas características los dispositivos móviles se han convertido en objeto de crímenes y actos ilícitos.

2.2.2. Evidencia digital

En informática forense la evidencia digital o prueba electrónica es uno de los términos más destacados y se la puede definir como la información que se encuentra almacenada o transmitida [13]. Para que la evidencia digital tenga validez probatoria debe ser: admisible, auténtica, completa, creíble, segura y confiable. Según ISO/IEC 27037:2012 [13], la evidencia digital, se conoce como: " información o datos, almacenados o transmitidos de forma binaria que pueden ser tomado en cuenta como evidencia o prueba".

Como se ha mencionado a lo largo del capítulo, la evidencia digital es la materia prima para cualquier investigación forense, entonces se debe tener un protocolo de actuación que se debe seguir durante toda la vida útil de la evidencia digital, es decir desde el instante que se obtiene los datos hasta que se destruye o ya no es relevante para la investigación. A ésto se lo conoce como (Cadena de Custodia (CdC)) [21]. Este procedimiento debe ser riguroso, tanto con las pruebas, los hechos, así como también con el personal que tiene acceso a la evidencia. Mientras que, la línea temporal o línea de tiempo es fundamental para indagar la información requerida en base a un criterio de tiempo determinado que es útil para la investigación. Cualquiera que sea el análisis se debe crear una línea temporal, es decir, los acontecimientos o actividades que el dispositivo ha tenido en manos de su propietario o propietarios [18].

2.3. Dispositivos móviles

Martin Cooper es una de las primeras personas en desarrollar la tecnología para teléfonos móviles y se lo considera como el "padre de la telefonía celular", ésta fue la catapulta para el desarrollo y lanzamiento de nuevas tecnologías móviles; desde sistemas analógicos conocidos como de primera generación a sistemas digitales llamados de segunda generación [22]. Los usuarios harían uso no sólo de servicio de voz y mensajería, sino de otros servicios de acceso a redes, acceso a Internet, servicio de video conferencia, etc. Esto hizo que los sistemas de tercera generación incrementaran el ancho de banda de las redes celulares y proporcionarán una amplia gama de servicios avanzados y mejor capacidad, mientras que los sistemas de cuarta generación son una extensión de la tecnología 3G pero con la diferencia de mayor ancho de banda y aumento de servicios [23].

Debido al avance tecnológico en los sistemas de los dispositivos móviles, cada vez son más compactos y sofisticados, entonces se podría definir a un dispositivo móvil como: un pequeño dispositivo de computación portátil, con conexión permanente o intermitente a una red, con memoria limitada, con funciones generales [24]. En su mayoría los dispositivos tienen un SO-móvil donde se pueden ejecutar aplicaciones, las cuales permiten que dichos dispositivos sean

utilizados para juegos, multimedia, navegadores, agendas y más.

2.3.1. Sistema Operativo

Un Sistema Operativo (SO) es el *software* principal, es un conjunto de órdenes y programas que gestionan los procesos básicos y los recursos de *hardware* de un dispositivo. Existen SO como Windows, Linux y MAC OS para ordenadores, mientras que para los dispositivos móviles como por ejemplo teléfonos inteligentes (*smartphone*), tabletas, reproductores, etc son mucho más simples y se los conoce como Sistema Operativo móvil (SO-móvil), están directamente orientados a la conectividad inalámbrica y necesidades específicas. Es una plataforma de *software* sobre la cual otros programas llamados aplicaciones se pueden ejecutar, el SO-móvil es menos robusto que el SO para computadores de escritorio o portátiles [24]. El proceso de evolución y los avances tecnológicos han dado una variedad de SO-móvil que compiten en el mercado, algunos de éstos se describen en las siguientes sub-secciones.

2.3.2. Android OS

Android es un SO, diseñado originalmente para dispositivos móviles inteligentes, basado en el *kernel* de Linux. Este SO originalmente pertenecía a la compañía Android Inc., pero hoy en día su dueño es Google ya que fue comprado en 2005. El objetivo de Google fue que Android sea un espacio de código abierto *Apache License* para generar y desarrollar *software* en dicha plataforma [3]. Desde 2011, Android tiene la mayor base instalada de cualquier sistema operativo móvil y se han vendido más ejemplares que otros dispositivos Windows, iOS y Mac OS combinados a partir de 2013. También la tienda de *Google Play* tuvo más de un millón de aplicaciones de Android publicadas y más de 50 mil millones de aplicaciones descargadas [24].

La plataforma además de ser un sistema operativo móvil, también proporciona una máquina virtual personalizada (Máquina virtual Dalvik DVM), de esta manera, las aplicaciones se ejecutan y actúan como middleware entre el código y el sistema operativo [3].

Arquitectura Android

Como se mencionó anteriormente, Android OS utiliza un Kernel de Linux con la Interfaz de Programación de Aplicaciones (API) de alto nivel escrito en C, las aplicaciones se programan en Java y ejecutan con la Máquina Virtual Dalvik (DVM) [24]. Como se puede ver en la Figura 2.1, la arquitectura se encuentra formado por capas. Las capas se encuentran interrelacionadas entre ellas ya que cada una utiliza servicios de las capas anteriores y de forma inversa da sus servicios a las capas superiores [2]. La capa base de la arquitectura es el Kernel de Linux, debido

a la potabilidad y flexibilidad.

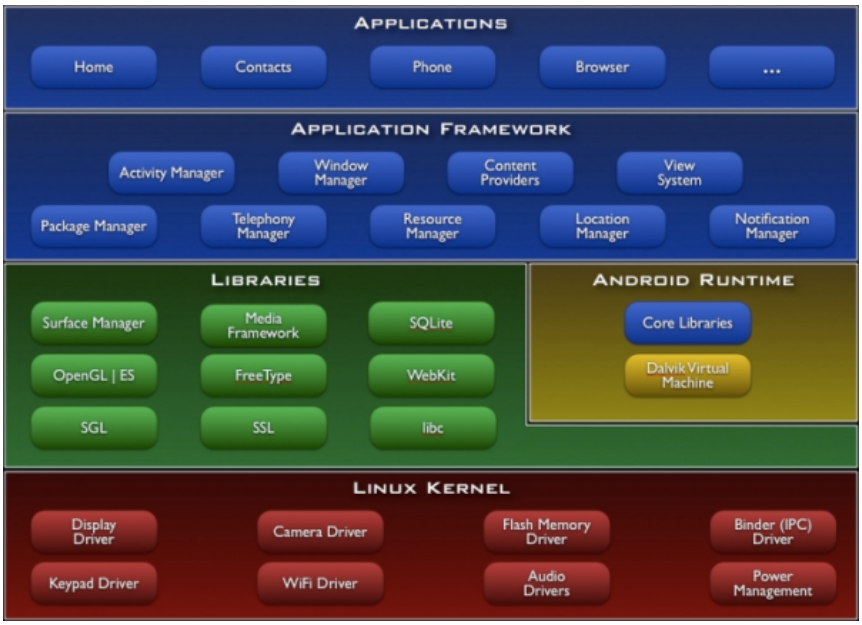


Figura 2.1: Arquitectura Android. Fuente [2]

2.3.3. iOS

Es un SO de Apple (antes iPhone OS) exclusivamente para sus dispositivos móviles iPhone, iPod touch, iPad y Apple TV, vio la luz en 2007 con la salida al mercado del primer teléfono móvil. iOS es una variante del Mac OS X, comparte su fundamento básico que es un código POSIX compatible con UNIX OS [24].

Arquitectura iOS

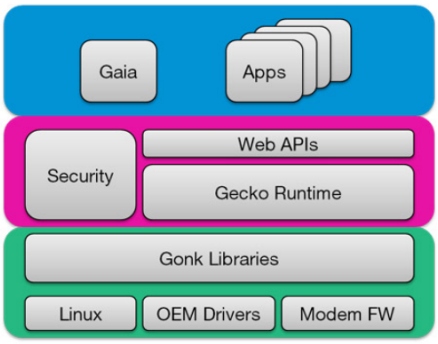


Figura 2.2: Arquitectura iOS. Fuente [3].

El SO de Apple se basa en cuatro capas de abstracción: *Core OS, Core Services, media, y Cocoa Touch* como se observa en la Figura 2.2. Las capas de nivel superior sirven como intermediarias entre las aplicaciones y el hardware del dispositivo. Las capas superiores se basan en las capas inferiores, donde las capas inferiores poseen el control de los servicios básicos. Las aplicaciones son escritas en Objective-C utilizando *Cocoa Touch* como biblioteca principal. *Objective-C* es una extensión del lenguaje C y *Cocoa Touch* es una colección de clases [3].

2.3.4. Windows phone

Windows Phone, al comienzo de sus días llamado Windows Mobile, es un SO desarrollado por Micrososft que apunta a dispositivos inteligentes y *Pocket PC*. En 2010, Microsoft anunció el desarrollo de Windows Phone para reemplazar a Windows Mobile y fue lanzado oficialmente al mercado, desarrollado para teléfonos inteligentes y otros dispositivos móviles [24].

2.3.5. BlackBerry OS

BlackBerry OS fue desarrollado por *Research In Motion* (RIM) exclusivamente para dispositivos BlackBerry y dispositivos tablet. BlackBerry OS se ejecuta en variantes de dispositivos Blackberry como: *Bold, Curve, Pearl y Storm*. Este SO es mayormente conocido por su soporte para correo electrónico corporativo y sus protocolos compatibles son: *Mobile Information Device profile* (MIDP) de Java y WAP, que se sincronizan a través de un servidor *BlackBerry Enterprise Server* (BES). Otra característica de BlackBerry OS proporciona un método para el acceso a Internet por medio de *BlackBerry Internet Service* (BIS).

A diferencia de los SO Android y Windows Phone, que pueden ejecutarse en diversas marcas de móviles; el sistema operativo BlackBerry al igual que iOS se puede ejecutar solo en teléfonos BlackBerry.

2.3.6. Estadísticas

En Ecuador, cada año se incrementa la cantidad de población que posee dispositivos móviles debido a su capacidad de procesamiento y la facilidad de realizar una serie de actividades. Mediante los estudios realizados por el Instituto Nacional de Estadística y Censo (INEC) [4] hasta 2016, cada año se aumenta la cifra de usuarios que poseen dispositivos celulares. Como se observa en la Figura 2.3 la población ha ido migrando de la telefonía fija a telefonía celular llegando a un 90.1 % en 2016.

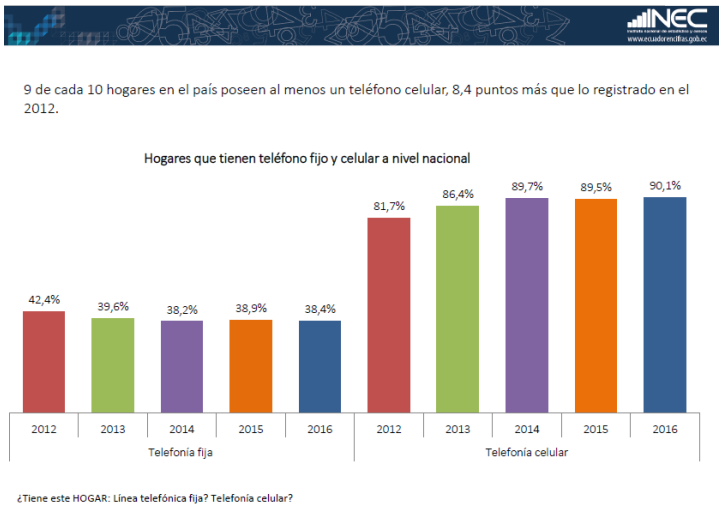


Figura 2.3: Usuarios a nivel nacional de celulares. Fuente INEC [4].

Por otra parte, en la Figura 2.4 se han desglosado los porcentajes según las provincias teniendo a la provincia de Azuay en quinto lugar con un porcentaje de 57.5 %, es decir, más de la mitad de la población posee como mínimo un teléfono celular activado.

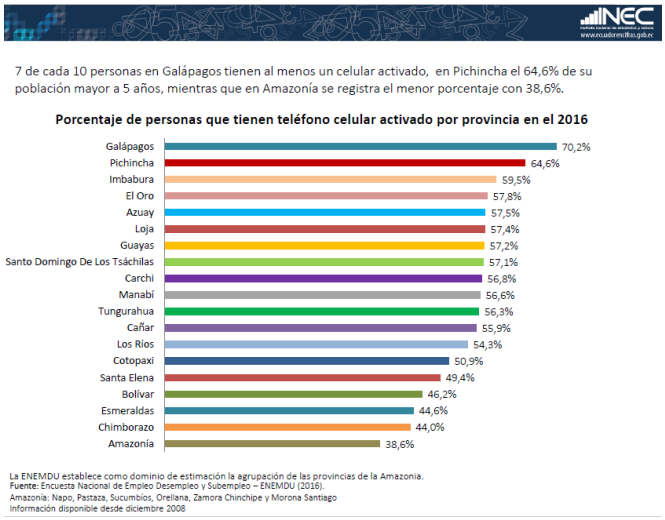


Figura 2.4: Usuarios por provincia que poseen telefonía celular. Fuente INEC [4].

Debido al avance tecnológico, no sólo la población ha optado por telefonía celular, sino a celulares de alta gama conocidos como teléfonos inteligentes (*smartphone*). En la Figura 2.5 la INEC da a conocer que el 52.9 % de la población posee un teléfono inteligente [4]. La INEC [4] también presenta resultados de cómo utilizan los usuarios sus teléfonos, donde se observa que

la mayoría de personas le da un uso para acceder a sus redes sociales, Internet o correos.

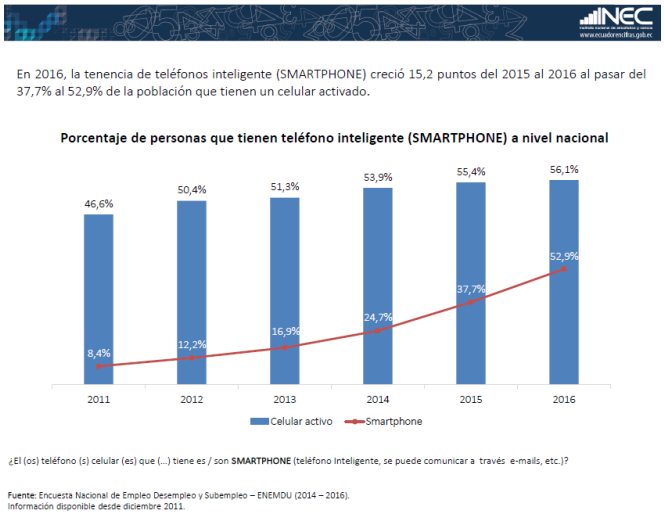
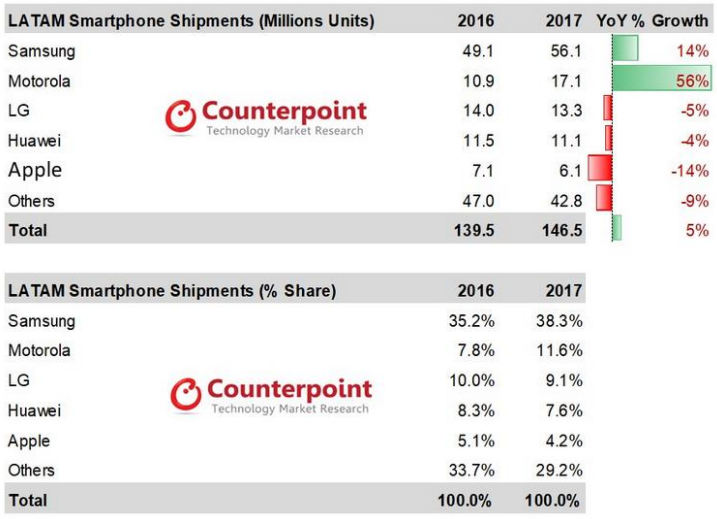


Figura 2.5: Usuarios a nivel nacional que poseen teléfonos inteligentes. Fuente INEC [4].

Hoy en día, existen varias marcas de teléfonos celulares debido a la gran demanda de los usuarios. El centro de investigación *Counterpoint* [5] determina que en el año 2017, las marcas con mayor acogida por su accesibilidad y precios son Samsung seguido por Motorola con un crecimiento en sus ventas como se observa en la Figura 2.6. Finalmente LG, Huawei y Apple poseen un menor porcentaje de ventas. Estas marcas líderes tienen como SO Android que según Chernyshev et al., en [8] explican que es un líder del mercado dominante.



LATAM Smartphone Shipments (Millions Units)	2016	2017	YoY % Growth
Samsung	49.1	56.1	14%
Motorola	10.9	17.1	56%
LG	14.0	13.3	-5%
Huawei	11.5	11.1	-4%
Apple	7.1	6.1	-14%
Others	47.0	42.8	-9%
Total	**139.5**	**146.5**	5%

Counterpoint Technology Market Research

LATAM Smartphone Shipments (% Share)	2016	2017
Samsung	35.2%	38.3%
Motorola	7.8%	11.6%
LG	10.0%	9.1%
Huawei	8.3%	7.6%
Apple	5.1%	4.2%
Others	33.7%	29.2%
Total	**100.0%**	**100.0%**

Counterpoint Technology Market Research

Figura 2.6: Marca de celulares con mayor demanda. Fuente [5].

2.4. Estándares, normas, regulación y seguridad

Actualmente los procesos para el análisis forense, no están estandarizados, es decir, no siguen pautas descritas por un documento ya sea nacional o internacional. Existen organizaciones que proporcionan guías, consejos y mejores prácticas para minimizar errores en la investigación; como son: Internet Engineering Task Force (IETF), Asociación Española de Normalización y Certificación (AENOR) o International Organization for Standardization (ISO) y International Electrotechnical Commission (IEC), así como la policía y departamentos de justicia de varios países proponen varios documentos.

2.4.1. Regulación estatal

En la actualidad, las nuevas tecnologías y la informática está avanzando de manera exponencial. La combinación de delincuencia con la accesibilidad de estas tecnologías ha dado como respuesta la generación de nuevas sanciones penales de acciones relacionadas con la informática [25]. Cada país aplica sanciones cuando el delito ha sido cometido dentro del territorio nacional, Temperini [25] lista los delitos informáticos de la siguiente manera:

- Violación de datos personales.
- Difusión de *malware*.
- Hurto informático.
- Difusión maliciosa de información.
- Suplantación de identidad digital.
- *Grooming*.
- Captación o venta ilegítima de datos.
- *Carding*.
- Espionaje informático.
- Violación a la intimidad.

Según Temperini [25], en 2014 Ecuador tiene tan solo 36 % de estadísticas sobre el nivel de sanción penal de los delitos anteriormente listados; también no existen regulaciones o normativas sobre algunos agravantes anteriormente mencionados.

En Ecuador los delitos informáticos empezaron a ser penalizados en el año 2002 en el proyecto para la creación de la ley de comercio electrónico, esta ley ya se había propuesto en el año 1999, posteriormente se los incluyeron en el Código Penal [26].

Delitos informáticos penalizados en Ecuador

Los delitos informáticos o ciberdelitos es toda aquella actividad ilícita para el robo de información a través de dispositivos. En el Código Orgánico Integral Penal (COIP) [16, 27] se especifican estas clases de acciones desde los artículos 229 al 234 y el artículo 500, de la sección tercera sobre los delitos contra la seguridad de los activos de los sistemas de información y comunicación. Según COIP [16, 27] son sancionados los delitos como:

- **Arts. 173 y 174:** Acoso sexual y la oferta de servicios sexuales con menores de edad.
- **Arts. del 190 al 194:** Apropiación fraudulenta de información y dinero a través de medios electrónicos.
- **Art. 191:** Reprogramación o modificación de información de equipos terminales móviles como tablets, celulares entre otros.
- **Arts. 194:** Comercialización ilícita de terminales móviles.
- **Arts. 212:** Suplantación de identidad.
- **Art. del 229 al 234:** Interpretación ilegal de datos hasta acceso no consentido a un sistema informático, telemático o de telecomunicaciones, transferencia electrónica de activo patrimonial, espionaje.
- **Art. 232:** Ataque a la integridad de sistemas informáticos.
- **Art. 234:** Acceso no consentido a un sistema informático entre otros.
- **Art. 500:** Hace referencia a todo lo que se considera como contenido digital.

Ley de comercio electrónico, firmas electrónicas y mensajes de datos [17]

El uso de sistemas de información y redes electrónicas, en donde se incluye el Internet son importantes para el desarrollo del comercio y la producción, tanto para sector público como para el sector privado. Ecuador debe contar con herramientas jurídicas que le permitan el uso de los servicios electrónicos.

Art. 1: El objeto de la ley. Es regular los datos electrónicos a través de redes de información, incluido el comercio electrónico y la protección a los usuarios.

Art. 2: Los principios generales. Reconocen a los mensajes de datos de igual importancia que los documentos escritos.

2.4.2. Estándares y normas internacionales

Además de la regularización nacional que se ha repasado se debe destacar las normativas y estándares internacionales más relevantes. Entre éstas están: ISO/IEC 27037, RFC 3227 y UNE 71505.

ISO/IEC 27037: Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence [13]

El estándar menciona los procedimientos que se deben seguir para analizar los distintos grupos de dispositivos como: computadores, periféricos, medios de almacenamiento digital, dispositivos de red, circuito cerrado de televisión, también menciona ciertos casos que pueden ocurrir al momento de asistir a la escena, como por ejemplo que el dispositivo esté encendido o apagado. Proporciona directrices en el escenario de la identificación, recolección, adquisición y preservación de la evidencia digital. De acuerdo a la norma, la evidencia digital está sostenida por tres principios: la relevancia, la confiabilidad y la suficiencia por lo que está orientada al proceso de la actuación pericial dirigidos a dispositivos actuales en el secuestro de la evidencia digital.

RFC 3227: Guidelines for Evidence Collection and Archiving [14]

Otra norma relacionada es la RFC 3227 publicado por la IETF. Este documento recoge directrices para recopilar y almacenar evidencias sin ponerlas en riesgo.

Esta norma proporciona las directrices necesarias para la recopilación y archivo de las pruebas en un incidente de seguridad, de esta manera se evita errores y la detección de ataques. También hace referencia a los procesos para la recolección de la escena, además de indicar la importancia de documentar y fotografiar cada proceso realizado; sin embargo, no indica las herramientas mínimas necesarias para acudir a la escena, prioriza el proceso de captura de estos datos y señala las maneras correctas de embalar las evidencias recolectadas.

UNE 71505: Tecnologías de la Información (TI). Sistema de Gestión de Evidencia Electrónica (SGEE). Parte 1: Vocabulario y principios generales [15]

Estas normas, publicadas por la Asociación Española de Normalización y Certificación tienen como finalidad dar una metodología para la preservación, adquisición, documentación, análisis y presentación de pruebas digitales.

Se establecen métodos para la gestión de *logs* de actividades que proporcionan información en un sistema de información. Esta norma es un marco referencia de buenas prácticas en la gestión de evidencia electrónica, cuyos principios son:

- Definir y describir los conceptos de seguridad de la información relacionados con las evidencias electrónicas.
- Identificar las relaciones entre el SGEE y el SGSI.
- Controlar de seguridad para la gestión de evidencias electrónicas.
- Describir los formatos de intercambio de las evidencias electrónicas y los mecanismos técnicos aplicables, para el mantenimiento de su confiabilidad.

2.5. Herramientas

Actualmente existen gran variedad de aplicaciones para el análisis forense que trabajan sobre diversos aspectos del dispositivo móvil, por ejemplo, sobre memoria interna, aplicaciones, mensajes, etc. Existen los llamados *suites* que toman todos los puntos anteriores y los unen en un solo análisis creando una herramienta potente y útil [18].

Las ventajas de utilizar herramientas forenses de código abierto (*open sourse*) para una investigación forense además de ser gratuitas, pueden ser examinadas ante el tribunal y comprobar que éstas no alteren la evidencia. También se emplea herramientas de tipo comerciales ya que éstas proporcionan una gran variedad de alternativas para el análisis [28].

En la siguiente sub-sección se presentan las herramientas que van a ser utilizadas.

2.5.1. Herramientas comerciales

Oxygen forensic suit [29]

Es un *software* forense comercial diseñado especificamente para el análisis lógico, búsqueda de pruebas en dispositivos móviles y presentación de informes. La herramienta posee la capacidad de extraer información de contactos, calendario, mensajes, imágenes, videos, aplicaciones entre otros archivos. También tiene la capacidad de recuperar una amplia variedad de datos borrados. Genera informes en archivos como PDF, RTF, XLS, XML, etc.

MOBILedit [30]

Es una herramienta de tipo comercial reconocida por el Instituto Nacional de Estándares y Tecnología. Ayuda a la extracción del contenido de dispositivos móviles por medio de los puertos USB, Bluetooth e Infrarrojo. Los datos adquiridos son almacenados en formato med, adicionalmente posee la capacidad de acceso a los datos de IMEI del dispositivo para ser registrados, de esta forma comprobar si estos han sido reportados como robados. Finalmente genera reportes en Word, XSL, navegador, XML.

Andriller [31]

Andriller es una aplicación de tipo comercial que contiene un conjunto de herramientas de adquisición de datos no destructiva, es capaz de descifrar contraseñas como patrón y PIN para dispositivos Android, algunos dispositivos iOS y Windows. Genera reportes de alto nivel en formato HTML y Excel.

2.5.2. Herramienta código abierto

Autopsy [32]

Es una de las herramientas gratuitas más completas y utilizadas, posee un conjunto de aplicaciones útiles. Permite un análisis de la línea de tiempo para identificar la actividad y analiza el registro del sistema operativo Windows. Otras de las características es la extracción datos EXIF de las imágenes, visualización de miniaturas de las mismas y clasificación de los archivos del sistema por tipo, entre varias opciones y herramientas.

Bulk Extractor [33]

Es un *software* de código abierto y se lo define como "cavando datos en asteroides" (*Data carving on asteroids*). La herramienta se la puede usar en SO Windows, Linux y MAC OS X. Posee la capacidad de recolección y análisis de datos, automáticamente clasifica estos datos según el tipo de información ya sea correos, teléfonos, contraseñas, etc. Se distingue de otras herramientas por su velocidad y minuciosidad.

Kali Linux [34]

Es una de las herramienta basada en Linux más completa para realizar análisis forense, entre sus características, ésta ofrece un entorno de trabajo orientado a las fases de análisis forense, una interfaz gráfica amigable y un proceso que genera informes a partir de los resultados. Se organiza en diferentes categorías para de esta manera facilitar la búsqueda de herramientas para la investigación. Según la FundaciónOWASP [35], recomienda las siguientes herramientas para el análisis forense, creación de imágenes, suites, RAM dentro de este entorno: i) binwalk, ii) Chkrootkit, iii) foremost, iv) galleta, v) voltafox, y vi) volatility. Todas estas herramientas se ejecutan en la terminal mediante línea de comandos.

MD5Summer [30]

MD5Summer es un programa originario para SO Unix que tiene versiones para diferentes plataformas. Tiene la capacidad de realizar sumas de comprobación MD5 de un fichero o una carpeta entera y almacena los resultados en un archivo texto, esta función devuelve un *hash* único para cada archivo. Al ser modificado un archivo éste devuelve un *hash* totalmente diferente, lo que ayuda a verificar la integridad de los datos.

hashdeep [36]

Es una herramienta recursiva gratuita que permite crear y comprobar ficheros, trabaja con SHA1, SHA2, Tiger y Whirlpool. Ésta crea un fichero maestro, el cual se verifica para comprobar

si hubo cambios en los ficheros existentes. El modo de auditoría con el que trabaja este programa permite identificar archivos nuevos, modificados, movidos y perdidos. Este programa existe para SO Windows y la mayoría de los sistemas basados en Unix, incluido OS X.

Android SDK (Software Development Kit) [37]

Es un kit de herramientas para el desarrollo de aplicaciones el cual se ejecuta como un emulador del sistema Android, la manera de interactuar a nivel de consola es mediante el depurador Android Debug Bridge (ADB), que es un juego de herramientas incluido en el paquete SDK de Android. ADB se conecta vía USB en la máquina que se va a analizar. Las plataformas de desarrollo son: GNU/Linux, Mac OS X y Windows.

2.5.3. Análisis de las herramientas

Se realiza un tabla comparativa de las diferentes herramientas para la extracción de información mencionadas, sus características y plataformas, como se puede observar en la Tabla 2.1.

Tabla 2.1: Análisis comparativo

Herramienta	Adquisición	Análisis	Reporte	Características	Plataforma
Oxygen Forensic	x	x	x	-Extrae información básica del móvil, SIM, memoria volátil, navegador web. -Protección de integridad de datos. -Obtención de *backup* e imagen forense.	Windows
MOBILedit	x	x	x	-Análisis de teléfonos mediante cable, bluetooth, infrarrojo. -Recolección de agenda, llamadas, mensajes, carpetas de archivos, multimedia. -Obtención de *backup*.	Windows
Andriller	x		x	-Adquisición de datos y copia de seguridad. -Descifrar contraseñas. -Desencriptado de base de datos de WhatsApp. -Informes HTML y XLS.	Windows/ Linux
Autopsy		x	x	-Crear notas del especialista. -Visor de miniaturas que muestra las imágenes. -Genera informes en HTML, XLS, tex.	Windows/ Linux
Bulk extractor		x	x	-Histograma de características mas comunes. -Volcado de RAM. -Crear reportes en XML, tex.	Windows/ Linux/ MAC OS X
Kali Linux	x	x	x	-Incorpora Autopsy, binwalk, bulk_extractor, chkrootkit, foremost, galleta, volafox y volatility. -Utiliza herramientas para clonar dispositivos y romper contraseñas. -Analiza la RAM. -Genera informes a partir de los resultados.	Linux

Capítulo 3

Estado del Arte

En este capítulo se analiza el estado del arte a través de la elaboración de un mapeo sistemático, que permite determinar las aproximaciones sobre análisis forense en dispositivos móviles con sistemas operativos Android, tomando en cuenta los estudios más relevantes en este tema. En la sección 3.1 se platea el protocolo de revisión, realizando en la sección. La sección 3.2 se desarrolla la revisón de la literatura mediante sus tres fases: planificación, conducción y resultados. La sección 3.3 se presenta la información con mayor relevancia encontrados en los estudios primarios. Finalmente, la sección 3.4 se realiza una discusión de la revisión sistemática, también se discute las respuestas a las preguntas y sub-preguntas de investigación de la revisión sistemática.

3.1. Introducción

En los últimos años, se han reportado varias encuestas y revisiones destinadas al análisis de evidencia digital en dispositivos móviles [9, 38–40]. Kitchenham en [41] propuso una guía para revisiones sistemáticas donde existe tres fases: planificar, conducir y reportar la revisión. Una revisión sistemática de la literatura es un estudio secundario donde se evalúan, identifican e interpretan los estudios individuales denominados estudios primarios. En particular, Kitchenham et al., [42] plantea una metodología para la elaboración de revisiones sistemáticas, las mismas que siguen un conjunto de pasos rigurosos. El objetivo no es solo agregar toda la evidencia existente a una pregunta de investigación; sino también apoya el desarrollo de pautas basadas en evidencias para profesionales.

Mientras que, Sanchez et al., en [43] presentan un mapeo sistemático de las tecnologías desarrolladas con el uso de IUI, esta investigación se basa en la metodología de Kitchenham para revisiones sistemáticas y su participación en técnicas de ingeniería de software. Además, Cedillo et al., en [44] presentaron un estudio destinado a la revisión de un análisis forense en dispositivos móviles, también utiliza herramientas para un estudio de mapeo sistemático con el fin de categorizar y resumir la información en los últimos años.

Szvetits y Zdun en [45] realizan una revisión sistemática de la literatura (*Systematic Literature Review*)(SLR) con 3 fases que incluye: búsqueda inicial, filtro con criterios de selección definidos y una clasificación final. También este estudio analiza objetivos, técnicas, tipos y arquitecturas cuando se usan modelos en tiempo de ejecución. Mientras, Petersen et al., en [46] describen las diferencias entre la revisión sistemática y los estudios sistemáticos de mapeo. Estos autores caracterizan y resumen diez revisiones sistemáticas, en este estudio se encontró que los métodos difieren en objetivos, alcance y profundidad de los estudios.

Por otra parte, Petersen et al., en [47] intentan mejorar las guías para los mapeos sistemáticos, se analiza la práctica actual de los estudios de mapeo sistemático en ingeniería de software y propone actualizaciones a las mismas. Alherbawi et al., en [48] muestran una SLR con los siguientes temas: conjuntos de datos realistas, validación bajo almacenamiento de datos fragmentados y validación semántica para reducir las tasas de falsos positivos. Alharbi et al., en [49] presentan una SLR sobre procesos de investigación forense digital. Este estudio establece que los resultados SLR son reproducibles y hay una menor posibilidad de perder una referencia importante. Robinson y Clemens en [50] presentan una SLR para examinar y organizar los resultados de los estudios disponibles con respecto a los beneficios del aprendizaje-servicio identificados en la propuesta forense. La diferencia del presente estudio con respecto a todos los estudios previamente mencionados, se encuentra en las preguntas de investigación. En este documento, la pregunta de investigación se relaciona específicamente con evidencia digital en dispositivos móviles.

Aunque se han informado varias encuestas y revisiones relacionadas, éstas presentan dos limitaciones principales:

1. Se necesita un proceso más sistemático para resumir el conocimiento existente en el área forense aplicado a dispositivos móviles.
2. Existe la necesidad de realizar encuestas o revisiones, específicamente enfocadas en soluciones, para preservar, recopilar, validar, identificar, analizar e interpretar la evidencia digital.

3.2. Mapeo sistemático

La ciencia forense digital de los dispositivos móviles se ha convertido en un campo de estudio indispensable cuando se trata de crímenes; sin embargo, todavía es relativamente nueva, esto según [38]. Para una evaluación competente del tema de investigación, se realiza una revisión del estado actual a través del análisis de estudios primarios. Una revisión sistemática implica varias etapas y actividades [41, 42]:

- Planificación de la revisión
- Conducción
- Resultados

Este método de investigación ha ganado popularidad en los últimos años y ha sido adoptado en varios otros estudios relacionados con las ciencias de la computación y el campo de la ingeniería web [43].

3.2.1. Fase de planificación

Después de identificar la necesidad del mapeo, el mapeo sistemático se divide en seis pasos importantes que influirán en la investigación [41, 42]: i) Establecer la pregunta de investigación y las subpreguntas, ii) Definir la estrategia de búsqueda, iii) Seleccionar estudios primarios, iv) Evaluar la calidad, v) Definir la estrategia de extracción de datos y vi) Seleccionar los métodos de síntesis. La base de toda investigación es una pregunta general del tema que se denominará pregunta de investigación, es importante formular esta pregunta ya que es la base para empezar la investigación. Con la pregunta de investigación clara se puede formular las subpreguntas que son incógnitas que surgen en la revisión, conocidas también como preguntas secundarias.

Establecer la pregunta de investigación y las sub-preguntas

Pregunta de investigación: ¿Cuáles son las herramientas y métodos más populares para extraer, identificar, recopilar, preservar y administrar la evidencia de un dispositivo móvil?

Subpreguntas de investigación:

- **RQ1:** ¿Qué tipo de evidencia digital se puede encontrar en los dispositivos móviles para un análisis forense?
- **RQ2:** ¿Dónde se puede encontrar la evidencia digital en el dispositivo móvil?
- **RQ3:** ¿Qué herramientas se pueden utilizar para automatizar la recopilación y el análisis de evidencia digital?
- **RQ4:** ¿Cómo se evalúan las soluciones?

Definir la estrategia de búsqueda

Fuentes de datos y estrategia de búsqueda: se realiza una búsqueda manual de los trabajos relacionados con esta área y se han seleccionado los libros, revistas importantes, conferencias y talleres en el área forense, tal como:

- International Conference on Digital Forensics and Cyber Crime (ICDF2C).
- Systematic Approaches to Digital Forensic Engineering (SADFE).
- IEEE Security and Privacy Workshops.
- International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE).
- International Conference on Cybercrime Forensics Education and Training (CFET).
- International Journal of Electronic Security and Digital Forensics (IJESDF).
- IEEE Transactions on Information Forensics and Security.

Para realizar la búsqueda automática, las fuentes de información seleccionadas incluyen:

- ACM Digital Library.
- IEEEXplore.
- SpringerLink.
- ScenceDirect

Se ha seleccionado un conjunto de palabras clave, que permiten recuperar los documentos más relacionados. La cadena de búsqueda definida es: "*(FORENSIC) AND (HAND OR SMART OR MOBILE OR DEVICE) AND (DIGITAL) AND (EVIDENCE)*".

Período de búsqueda: La búsqueda se la seleccionó a partir de la aparición de las redes inalámbricas, Internet y dispositivos móviles que han ido evolucionando para adaptarse a las exigencias del usuario. La fecha que se eligió es 2007 debido a que fue el año donde se descargó la primera aplicación para teléfonos móviles [9]. Por lo que, solo se han considerado los estudios realizados después de esa fecha.

Selección de estudios primarios: Cada estudio procedente de las búsquedas automáticas y manuales han sido evaluadas para decidir si es incluido o excluido, inicialmente considerando su título, resumen y palabras clave.

Los criterios de inclusión para la selección del estudio son:

- Estudios que presenten métodos para identificar, recolectar, preservar, analizar y presentar evidencia en dispositivos inteligentes.
- Estudios que presenten herramientas que permitan automatizar el proceso forense.
- Estudios que presenten métodos que nos permitan salvaguardar la evidencia digital.

Los criterios de exclusión seleccionados son:

- Estudios introductorios para problemas específicos, libros y workshops.
- Estudios duplicados en diferentes repositorios de información.
- Estudios cortos de menos de cinco páginas.
- Estudios que no hayan sido escritos en inglés o español.

Evaluación de calidad

Además de los criterios generales de inclusión/exclusión, se considera fundamental evaluar la "calidad" de los estudios primarios [41, 42], también Cedillo et al., en [44] utilizó un cuestionario de escala de Likert de tres puntos para proporcionar una evaluación de calidad de los estudios seleccionados. El cuestionario contiene los siguientes aspectos:

- Información forense relacionada con la recopilación, gestión y preservación de la evidencia encontrada en dispositivos móviles.
- Revista o conferencia en la que se publicó el documento (por ejemplo, revista, actas, clasificación principal).
- Si el estudio ha sido citado por otro autor (Google Scholar).

El puntaje para cada pregunta cerrada es la media aritmética de todos los puntajes individuales de cada revisor. La suma de las tres puntuaciones de preguntas cerradas de cada estudio pro-

Tabla 3.1: Preguntas de investigación

RQ1: ¿Qué tipo de evidencia digital se puede encontrar en los dispositivos móviles para un análisis forense?		
EC1	Artefactos	Indicadores de navegación Historial de navegación Archivos temporales Otros
EC2	Origen de la evidencia	Navegadores Aplicaciones Red Registros Multimedia Proceso del sistema
RQ2: ¿Dónde se puede encontrar la evidencia digital en el dispositivo móvil?		
EC3	Perspectiva	Dispositivo del cliente Tránsito
EC4	Artefactos locales	Historial de navegación Archivos temporales (cache, cookies, etc)
EC5	Tipos de sesión	General Sesión privada/incógnita Sesión portable
EC6	Dispositivos finales	Teléfonos inteligentes Otros dispositivos
RQ3: ¿Qué herramientas se pueden utilizar para automatizar la recopilación y el análisis de evidencia digital?		
EC7	Dependencias	Software Métodos
RQ4: ¿Cómo se evalúan las soluciones?		
EC8	Métodos de evaluación	Caso de estudio Experimento controlado Prueba de concepto

porciona un valor final que no se utiliza para excluir artículos del estudio de mapeo sistemático, mas bien se usa para detectar estudios representativos.

Definición de la estrategia de extracción de datos

La estrategia de extracción se basa en las posibles respuestas de las subpreguntas que fueron definidas en la sección 3.2.1. Asegura la misma extracción de criterios para todos los estudios y facilita la clasificación de los mismos. La Tabla 3.1 muestra de manera detallada la extracción de datos y categorización de los estudios.

Selección de métodos de síntesis

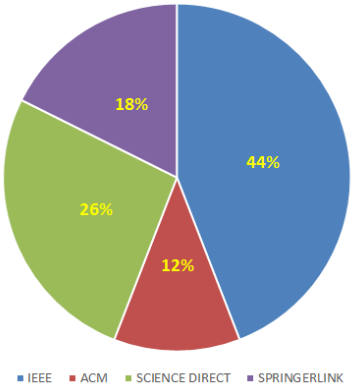


Figura 3.1: Porcentaje de estudios aceptados clasificados por las bibliotecas digitales.

Se han aplicado tanto métodos cuantitativos como cualitativos. La síntesis de los métodos cuantitativos está basada en:

- La contabilización los estudios primarios que han sido clasificados en cada respuesta de nuestras sub-preguntas de investigación.
- La contabilización del número de estudios encontrados en cada una de las fuentes bibliográficas.
- Las síntesis cualitativas están basadas en incluir varios estudios representativos para cada sub-pregunta considerando los resultados de la evaluación de calidad.

3.2.2. Fase de conducción

Luego de la búsqueda para identificar los estudios primarios en las diferentes bibliotecas seleccionadas, la aplicación del protocolo de revisión y los criterios de inclusión, se seleccionaron 34 estudios primarios de 931 como se muestra en la Figura 3.1.

3.2.3. Reporte de resultados

La estrategia de extracción de datos se definió dividiendo cada pregunta de investigación en un criterio más específico y se establecen criterios de extracción. Con respecto a la pregunta RQ1 el tipo de evidencia con mayor relevancia en los estudios son los registros y aplicaciones. Estos afirman que se han desarrollado más investigación sobre estos ítems como se observa en la Figura 3.2.

Con respecto a la pregunta RQ2, se puede denotar que los estudios se centran principalmente en

dispositivos móviles y los datos que se extraen se encuentran en archivos y registros temporales. Si bien la pregunta RQ3 depende del tipo de plataforma que se utiliza para extraer la evidencia, entre los documentos estudiados con respecto a la plataforma, se mencionan varias herramientas tanto para hardware y software que dependen del tipo de datos que se analizarán.

Finalmente, en la pregunta RQ4, las metodologías dadas en los diferentes ítems tienen un gran porcentaje de experimentos controlados y pruebas de conceptos, que pueden realizarse para demostrar la factibilidad de los estudios primarios. Estos experimentos controlados son diseñados por los autores para dar validez a los resultados obtenidos.

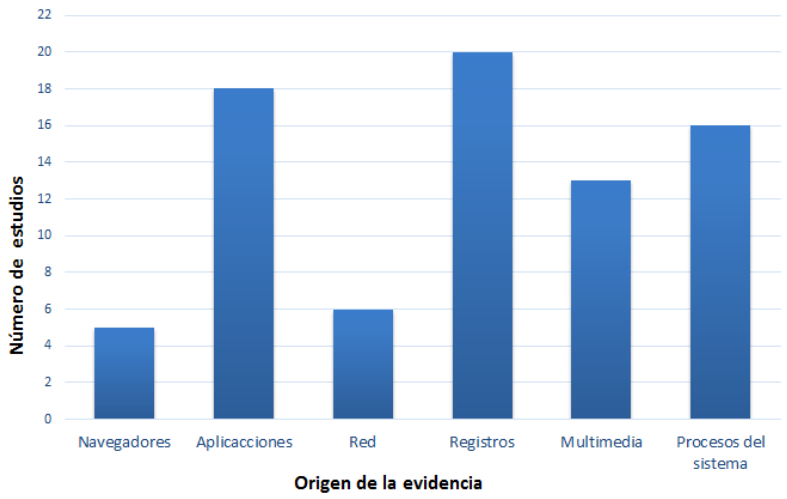


Figura 3.2: Porcentaje de estudios clasificados por origen de la evidencia.

En la Tabla 3.2 se muestra los porcentajes de los estudios según las preguntas más relevantes para la investigación.

Tabla 3.2: Resultados del mapeo sistemático

Código	Subpreguntas de investigación	Posibles respuestas	# Estudios	% Porcentaje
RQ1: ¿Qué tipo de evidencia digital se puede encontrar en los dispositivos móviles para un análisis forense?				
EC2	Origen de la evidencia	Navegadores	5	6.02
		Aplicaciones	18	21.69
		Red	6	16.66
		Registros	20	55.55
		Multimedia	13	36.11
		Proceso del sistema	16	44.44
RQ2: ¿Dónde se puede encontrar la evidencia digital en el dispositivo móvil?				
EC4	Artefactos locales	Historial de navegación	6	16.67
		Archivos temporales	26	72.22
		(cache, cookies, otros)	27	32.53
EC6	Dispositivos finales	Teléfonos inteligentes	30	83.33
		Otros dispositivos	19	52.78
RQ3: ¿Qué herramientas se pueden utilizar para automatizar la recopilación y el análisis de evidencia digital?				
EC7	Dependencias	Software	30	83.33
		Métodos	5	13.89
RQ4: ¿Cómo se evalúan las soluciones?				
EC8	Métodos de evaluación	Caso de estudio	2	6
		Experimento controlado	18	50
		Prueba de concepto	15	42

3.3. Discusión de resultados

En esta sección de resultados, se presentan los temas más relevantes encontrados en los estudios primarios, que fueron seleccionados para este mapeo sistemático. Estos temas se los clasifica de la siguiente forma: i) Origen de la evidencia, ii) Metodologías de evaluación, iii) Herramientas y software para la extracción de evidencia digital, iv) Plataformas y v) Aplicaciones.

3.3.1. Origen de la Evidencia

En el área de investigación forense existen aspectos legales que no se cumplen, estos aspectos implican el uso indebido de aplicaciones, fraude, robo, difusión de materiales con derechos de autor, etc. Taylor et al., en [12] analizan los procesos para obtener evidencia digital, es decir, procedimientos de investigación forense por computadora, adquisición de evidencia digital desde aplicaciones de telefonía móvil y aspectos legales. Además, este estudio explica que si se obtienen datos personales en una investigación, esta información debe ser accesible solamente para el equipo de investigación. Además, todos los datos enviados, descargados y guardados dejan un recorrido que se borra, esto se llama huella [51], significa que siempre hay evidencia sobre las acciones realizadas dentro del teléfono inteligente. "El Principio de intercambio de Locard" (como cita Zatyko y Bay en [52]) establece que "cada contacto deja una huella", este principio también es relevante para las investigaciones forenses.

Además, existen diferentes tipos de evidencia digital (por ejemplo, imágenes, videos, mensajes multimedia, archivos, metadatos de archivos, registros, correos electrónicos). Depende de los investigadores y de la información que desean extraer. Aun así, varios estudios [9, 10, 38, 40, 51, 53–60] se centran en aplicaciones de mensajería instantánea. Extraen información de diferentes fuentes (por ejemplo, mensajes eliminados, imágenes, videos, voz/video en vivo, llamadas). El tipo de información podría ser, ya sea en la RAM o en la ROM [61, 62]. También se puede extraer de la tarjeta SIM, que debe analizarse inmediatamente después de la memoria interna, mientras el dispositivo todavía está encendido [63].

Mylonas et al., en [64] dividen la evidencia según su fuente como: datos de mensajes, datos del dispositivo, datos de la tarjeta SIM, historial de uso, datos de la aplicación, datos del sensor, datos de entrada del usuario. Por otra parte, Mylonas et al., en [65], presentan consideraciones de seguridad como eludir permisos, en el cual los usuarios son delegados para otorgar privilegios de administrador cuando se va a instalar una aplicación. Otras consideraciones presentadas eluden las notificaciones visuales para proteger sensores, como la cámara y el GPS, a través de notificaciones visuales y finalmente el modelo de seguridad de Android, que no distingue entre mensajes de error, aplicaciones de terceros y aquellos creados por SO. Esta falla ayuda al malware a engañar a los teléfonos inteligentes.

Por otra parte, los autores de [39, 53, 66], examinan y analizan las carpetas de los dispositivos que contienen información de las aplicaciones de las redes sociales como es la caché y bases de datos. Estas pruebas pueden ser fotos, videos, aplicaciones, mensajes o registros. Como se sabe, hay varias aplicaciones para las diferentes ramas existentes. En Ntantogian et al., en [67] afirman que las aplicaciones que se consideran son: banca móvil, compras electrónicas/financieras, administrador de contraseñas, finalmente cifrado y ocultación de datos. Dichos escenarios se establecen mediante la creación de usuarios y contraseñas en un dispositivo Android como datos

en movimiento y en función de la funcionalidad proporcionada de cada aplicación. Para obtener la información de la memoria volátil del teléfono, se evaluará la privacidad, en particular, si se puede descubrir la autenticación de las credenciales.

3.3.2. Metodología de evaluación

Scrivens y Lin en [38] diseñaron una metodología basada en 3 pasos: i) ubicación de almacenamiento de datos, ii) extracción de datos y iii) análisis de datos. En primer lugar, es necesario conocer la ubicación de los datos que se van a extraer con la autorización correspondiente, también es necesario contar con los permisos adecuados para priorizar la integridad de los datos. Más adelante, para realizar la extracción de datos, es necesario utilizar imágenes de recuperación de código abierto y otro software o hardware (por ejemplo, Chip-Off, suites de software forense y aplicaciones de respaldo). Varma et al., [61] utilizan imágenes no encriptadas que se evalúan con el método LIFTR que tiene 3 pasos: i) adquisición, ii) filtrado y iii) recuperación de datos con reproceso de datos. De manera similar, Mutawa et al., en [66], presentan tres etapas: i) escenarios, ii) adquisición lógica, y iii) análisis. Cabe señalar que todas esas metodologías se evalúan mediante experimentos controlados; el uso de ellos ayuda a corroborar los resultados de una manera sistemática. Un modelo básico para el proceso de una investigación forense fue descrito por los autores de [68]. Este modelo tiene ocho pasos, que son: i) identificación, ii) preparación, iii) preservación, iv) recolección, v) examen, vi) análisis, vii) presentación y viii) presentación de informes. De la misma manera, Kubi et al., en [69] presentan una metodología similar con seis actividades que son: i) recolección, ii) identificación, iii) adquisición, iv) preservación, v) examen y vi) informe. Luego, hay una metodología llamada Post-mortem, desarrollada por [70], porque todos los dispositivos no están en perfectas condiciones y algunos incluso se destruyen. Consiste en las nueve fases tradicionales, que son: i) identificación, ii) preparación, iii) preservación, (iv) adquisición, v) examen, vi) análisis, vii) informe, viii) presentación, y ix) revisión. Finalmente, Satrya et al., en [59] describen una metodología con cuatro pasos: i) identificar, ii) preservar, iii) analizar, y iv) presentar.

Mientras que, Anglano et al., en [55] estudian una metodología que no sigue los pasos específicos (ver diagrama de flujo de la Figura 1 de [55]), sino que es un diagrama de flujo que permite identificar, ubicar, analizar y ofrecer resultados aceptables. En síntesis, es un “análisis de código fuente"que analiza y determina el formato de los datos almacenados en carpetas. De forma similar, Mylonas et al., en [64], presentan un esquema que consta de 6 bloques: i) investigación, ii) selección de evidencia, iii) recolección de evidencia, iv) transmisión de evidencia, v) almacenamiento de evidencia y vi) terminación de investigación. Otra metodología, propuesta por Amato et al., en [71], tienen las siguientes fases: i) recopilación de datos, ii) representación ontológica, iii) razonamiento, iv) evaluación de reglas, y v) consulta. Este método se basa en la representación semántica, la integración y la correlación. Una representación ontológica ayuda

a las herramientas forenses y mejora las habilidades analíticas para correlacionar la evidencia más fácilmente. En contraste Cohen en [72], realiza una comparación entre dos modelos: el primero fue tomado de un estudio realizado por los autores caracterizados por requisitos legales, este modelo es bastante matemático ya que las variables se toman para obtener un resultado general. El segundo modelo es una alternativa al primero, la diferencia radica en el hecho de que los eventos son hipotéticos, pero también se basan en un contexto legal. Omeleze y Venter en [62], proponen un modelo genérico en el proceso de estandarización llamado Harmonized Digital Forensics Investigation (HDFI). Este modelo integra otros modelos estudiados por los autores y tiene acciones paralelas. Rahaditya et al., en [73] se centran en el Primer Taller de Investigación Forense Digital (DFRWS) que propone un proceso de investigación de siete fases que son: i)identificación, ii)preservación, iii)colección, iv)examinación, v)análisis, vi)presentación, vii)decisión.

Por otra parte, Tso et al., en [10], utilizan la metodología del proceso de copia de seguridad comparativa que se crea para los sistemas operativos iOS y utilizan la herramienta iTunes, donde básicamente comparan los archivos del dispositivo con la copia de seguridad. El método presentado por Husain y Sridhar en [57], comienzan con la creación de datos de prueba, seguido de la adquisición de datos desde el dispositivo iPhone y finalizando con el análisis de la información. Además, una de las metodologías más completas para iOS tiene seis pasos de acuerdo con [74]: i) preparación, ii) creación de información, iii) documentación y hashes, iv) captura de paquetes, v) ubicación y vi) comparación de nuevos datos con el dispositivo original. La mayoría de los documentos trata de la adquisición de información, pero en [75, 76] tienen una fase de preservación tradicional que implica la protección del sitio del evento y de la evidencia digital. Sin embargo, en datos desplegados en plataformas en la nube, la preservación física es posible solo si se puede acceder a los dispositivos. Por lo tanto, no hay otro tipo de preservación de datos para este tipo de plataformas, ya que los datos se almacenan en imágenes virtuales.

3.3.3. Herramientas y software para la extracción de evidencia digital

Scrivens y Lin en [38] analizan los métodos de software y hardware. En el campo de hardware, algunos de los métodos más populares son: *Chip-Off*, JTAG, Forensic Software Suites [77] , ADB. Además, hay herramientas habilitadas, como la presentada por [61], donde se desarrolla el método LIFTR, que utiliza motores de recuperación como Bulk_extractor [33]. Otras herramientas importantes presentadas por [40, 60, 63] son: FTK [78], Mobile Phone Examiner [77], Oxygen Forensic Suite [29], EnCase Neutrino, UFED [79]. En particular, Ntantogian et al., en [67] utilizan herramientas forenses de código abierto, que son muy útiles para el examen de la autenticación de credenciales. Otros estudios, como el realizado por Jahankhani y Azam, Kubi et al., en [69, 80] realiza revisiones sobre todas las herramientas que son útiles para la investigación forense en dispositivos móviles. Alyahya and Kausar en [53], muestran una com-

paración entre dos herramientas, AXIOM [81] y Autopsy [32], este experimento se realiza en una aplicación específica de Snapchat. Los resultados de este estudio muestran que la aplicación con la mejor herramienta es AXIOM, ya que recupera los artefactos de Snapchat con altos porcentajes. Yadav et al., en [68] presentaron una comparación entre seis herramientas forenses comerciales y de código abierto: EnCase, DFF [82], FTK [78], TSK [83], Helix [84] y Liveview [85]. Cabe descartar que cada herramienta está destinada al análisis de un tipo de evidencia en particular (imágenes, mensajes, aplicaciones, web, memoria volátil, etc)y dependiendo del tipo de evidencia y dispositivo se asigna la herramienta forense.

Tso et al., y Mutawa, et al., en [10, 66] analizan los datos a través de una aplicación patentada por *Apple Company.* iTunes no solo es un reproductor de audio y video, sino que también tiene la función de sincronización que puede hacer copias de seguridad. Otro punto a considerar según Mutawa et al., en [66] es la desactivación de la sincronización automática para conservar la integridad de la información, ya que impide el intercambio de información entre el dispositivo y la computadora. Mientras tanto, las herramientas Oxygen Forensics [29], Katana Forensics [86] y Elcomsoft [87] se utilizan para extraer evidencia de sistemas operativos basados en Android [74].

3.3.4. Plataformas

Hoy en día los sistemas operativos más populares son Android e iOS, cada uno con una arquitectura específica [8]. La arquitectura de iOS se basa en capas, donde las capas de nivel superior interactúan como intermediarios entre el *hardware* y las aplicaciones. Las aplicaciones se comunican a través de las interfaces del sistema, y ese mecanismo proporciona el desarrollo de aplicaciones que funcionan en dispositivos con diferentes capacidades de *hardware*. En contraste, Android es un sistema operativo basado en Linux que usa varias particiones para organizar las carpetas de archivos en el dispositivo y cada una con su propia funcionalidad.

Otros estudios [38, 53, 55, 61, 63, 67] aplican el análisis en dispositivos Android. En primer lugar, es importante conocer la ruta en la que se almacenan los datos, el tipo de privilegios otorgados y qué método y herramienta se pueden utilizar para la extracción de dichos datos. Los dispositivos Android utilizan un espacio aislado en el que se encuentran las aplicaciones y los datos del usuario y en el que los usuarios tienen su propia ubicación de almacenamiento [62].

Por otra parte, Anglano en [54], no usa un dispositivo, sino una plataforma de virtualización llamada YouWave. Esta plataforma emula un dispositivo Android. Aquí se crea una máquina virtual (VirtualBox), donde las aplicaciones se analizan con un emulador. Del mismo modo, Anglano et al., en [55], presentan una virtualización de dispositivos Android llamada AVD,

que actúa como un dispositivo físico real. En los dispositivos iOS, los investigadores deben considerar posibles opciones entre aquellos que limitan la visualización por ejemplo *Apple File Communication*, también aquellos en los que el acceso para ciertos archivos del dispositivo se encuentra en los medios y no son parte del sistema [10, 57, 63, 66].

Yates y Chi en [63], analizan otros sistemas operativos como Blackberry, que tienen dispositivos con sistema operativo o Windows Mobile, en los cuales la adquisición lógica no es posible; por lo tanto, el siguiente paso es la adquisición física.

3.3.5. Aplicaciones

Hay muchas aplicaciones para diferentes sistemas operativos (por ejemplo, Android, iOS, Linux y Windows Mobile). Algunos de los cuales se utilizan para llamadas y videoconferencias. Estas aplicaciones son útiles cuando se necesita realizar una investigación forense [53].

Otros estudios, como [9, 10, 38–40, 51, 53–60, 66] realizan un análisis forense en aplicaciones de mensajería instantánea, esto permite a los usuarios estar constantemente en contacto con otras personas para intercambiar información por ejemplo, números de teléfono, textos, video, imágenes y fechas. Sin embargo, hay casos en los que no hay datos relevantes para la inspección forense [10, 66]. Otro tipo de mensaje instantáneo es Snapchat, en los últimos años esta aplicación se ha vuelto más popular ya que es posible cargar archivos multimedia o mensajes, que están disponibles en línea por un período de 24 horas. Esta nueva tecnología ha sido un desafío cuando se requieren los datos generados [53]. En 2015, Walnycky et al., en [51] realizó un extenso análisis de 20 aplicaciones de mensajería social. Estas pruebas se realizaron en un entorno controlado, de esta forma se analizó el tráfico de la red desde el dispositivo cuando se enviaron los mensajes, ya sean de texto, video o imágenes.

Chen y Mao en [58] realizan un análisis forense en correos electrónicos. Para ejecutar la prueba experimental, usaron las herramientas MailMaster y QQMail y se enfocaron en la memoria volátil de los dispositivos Android. Por otro lado, Ovens y Morison en [74] realizan un análisis para iOS, este tipo de dispositivos tienen la aplicación Mail, y se investiga cómo funciona la transferencia del correo electrónico y los contactos de Apple entre un cliente y los datos de la nube. Shortall y Azhar en [60] presentan un estudio donde examinan los metadatos de los archivos adjuntos incluidos en los correos electrónicos. Mushcab y Gladyshev en [39] analizan las aplicaciones de redes sociales Instagram y Path; donde los resultados no fueron favorables ya que las copias de seguridad no revelan información fundamental.

Tso et al., en [10] tratan con Apple iTunes, que es principalmente una aplicación para computadoras; sin embargo, es una herramienta clave para extraer evidencia. Se administra direc-

tamente en la computadora a través de la administración de configuración de sincronización. Cuando se conecta a iTunes la información de resumen del dispositivo como el nombre del dispositivo, versión, número de serie, contactos, etc se descargan en la computadora. Anglano en [54] muestra que los mensajes y contactos se pueden reconstruir cronológicamente. Han sido intercambiados por los usuarios, pero en lugar de utilizar un dispositivo de mano, se reemplaza por un emulador del sistema operativo Android instalado en la computadora.

Este documento también tiene en cuenta las aplicaciones de almacenamiento implementadas en la nube: por ejemplo, Grispos et al., [88] estudian las aplicaciones de Dropbox y Box. Como resultado, se pueden tener archivos en la nube y los usuarios no realizan tareas de mantenimiento en la memoria caché, ya que dichos archivos no se eliminan. Además, Ovens y Morison [74] también dan un enfoque a los servicios en la nube donde encontraron que no hay hashes criptográficos consistentes.

Finalmente, hay análisis forenses en casos reales. Hajdarevic y Dzaltur en [89], analizan la información obtenida del correo electrónico, donde los pasos principales son la recopilación y el análisis de los datos de la red aplicados a una empresa. Cuando se refiere a dispositivos inteligentes manuales, no se trata solo de teléfonos celulares, iPad o tabletas, sino que podría ser cualquier otro dispositivo con conexión a Internet. Por lo tanto, hay varios dispositivos adicionales con conexión a Internet que pueden proporcionar información útil en una investigación forense. Harbawi y Varol en [90], discuten un modelo teórico de adquisición donde se propone el algoritmo de última instancia con siete pasos (inspeccionar incautados, recuperar evidencia digital, inspeccionar irregularidades, adquirir evidencia digital y producir copias de seguridad, incauta el dispositivo, restringe y realiza el informe). Finalmente, los mismos autores de [90] afirman que el área forense es aún joven y no hay una investigación extensa en este campo.

3.4. Discusión de la revisión sistemática

En la Figura 3.3 se puede apreciar la intersección del número estudios relacionados entre los principales criterios de extracción y es posible resumir, realizar y comprender las relaciones principales entre las preocupaciones y las características de forense para dispositivos móviles. Según el análisis sobre los artículos seleccionados se encontró que, en la categoría Origen de la evidencia, existe 17 estudios de aplicaciones en teléfonos inteligentes, mientras que en la categoría de artefactos locales hay otros 23 artefactos que son analizados por los autores (por ejemplo, caché, cookies, registros y memoria volátil, memoria no volátil) en el teléfono inteligente y 10 estudios se desarrollaron en los otros dispositivos (iPad, tableta, iPod) lo que concluye que el análisis forense esta orientado a dispositivos celulares.

Figura 3.3: Diagrama de burbujas.

Por otro lado, según el tema basado en las dependencias: en la categoría de origen de la evidencia el mayor desarrollo está orientado al tipo de *software* según el tipo de plataforma (Android, IOS, Linux, Windows Mobile). Finalmente, refiriéndose a los métodos de evaluación: la mayoría de los estudios son experimentos controlados, seguido de pruebas de concepto y por último dependiendo del tipo de evidencia y artefacto son casos de estudios.

Al término del presente capítulo las preguntas de investigación planteadas:

- **RQ1:** ¿Qué tipo de evidencia digital se puede encontrar en los dispositivos móviles para un análisis forense?
- **RQ2:** ¿Dónde se puede encontrar la evidencia digital en el dispositivo móvil?
- **RQ3:** ¿Qué herramientas se pueden utilizar para automatizar la recopilación y el análisis de evidencia digital?
- **RQ4:** ¿Cómo se evalúan las soluciones?

Las preguntas han sido respondidas en los diferentes apartados del reporte de resultados de la revisión de literatura.

RQ1, ha sido respondida en el apartado de origen de evidencia, donde varios de los autores identifican distintos tipos de evidencias como las que se encuentran en: navegadores, aplicaciones, red, registros, multimedia, procesos del sistema, provenientes de dispositivos móviles.

RQ2 de la misma forma, fue respondida en los apartados de plataformas y aplicaciones, se han

identificado los diferentes SO y aplicaciones móviles. Como SO principales se tiene Android, iOS, Windows Phone, cada uno deja posibles evidencias dependiendo del sistema de ficheros del SO. En cuanto a las aplicaciones, existe una innumerable cantidad disponibles en tiendas virtuales, pero los estudios se centran en aplicaciones de mensajería instantánea, correos electrónicos y almacenamiento en la nube.

RQ3 ha sido solventada en el apartado de herramientas y *software* para la extracción de evidencia, donde exponen distintas herramientas comerciales y de código abierto para la extracción de información en dispositivos móviles. Éstas se utilizan dependiendo de los datos que se van a extraer.

RQ4, esta pregunta fue abarcada en el apartado de metodologías de evaluación, donde se detalla varias metodologías propuestas y desarrolladas por los autores.

Si bien la revisión demuestra que existe una gran cantidad de estudios relacionados con el área forense en dispositivos móviles donde se emplea diferentes herramientas para la extracción de un elemento determinado. También muestra que, no existen estudios que compacten toda la evidencia extraída de un dispositivo móvil, obteniendo así un registro de todas las actividades que el usuario realiza en dicho dispositivo. Ésto se lograría con la utilización de varias herramientas forenses para la extracción de evidencia digital. Finalmente, se une toda esta información en un solo informe para la revisión del investigador.

Capítulo 4

Desarrollo del proceso

En este capítulo se trata el proceso de manera técnica, la parte de la seguridad, los ambientes elegidos y la proceso utilizado para la adquisición y su posterior análisis. En la sección 4.1 se da una introducción para el proceso forense, la sección 4.2 provee varias consideraciones para la investigación, la sección 4.3 delimita las fases de las que está compuesto el proceso, y finalmente, en las secciones 4.4, 4.5, 4.6 y 4.7 se detallan los pasos a seguir en cada fase de la investigación.

4.1. Introducción

Este capítulo esta dedicado al desarrollo del proceso que permite saber, ¿qué analizar?, ¿qué hacer?, ¿de qué manera actuar?, desde el instante que se retiene el dispositivo móvil para ser objeto de evidencia dentro de la investigación forense. Se ha desarrollado el proceso en 4 fases para el análisis. La primera fase es la identificación y preservación de la evidencia digital; la segunda fase es la adquisición del contenido del dispositivo; la tercera fase es el análisis en donde se pretende descartar la información irrelevante para la investigación; finalmente, en la fase cuatro se realiza el informe final de los hallazgos generados para ser plasmados de forma técnica.

4.2. Consideraciones

Al realizar un análisis forense se deben considerar algunos aspectos importantes que son de mucha ayuda para el personal y para la investigación forense digital.

- El proceso desarrollado es exclusivamente una fuente de ayuda para el perito forense, es decir que no es una medida para aplicar alguna leyes mencionadas en el capítulo 2, ni adiestramiento jurídico.
- Entender las características del dispositivo móvil, como la estructura y arquitectura del sistema Android.
- Adoptar las medidas necesarias por los investigadores para asegurar y preservar la evidencia, con el fin de no alterar la integridad de la información recolectada.
- Se deben considerar las leyes vigentes que se rigen en cada país, para disponer acciones, precauciones y por ende el cumplimiento de las mismas.
- Las herramientas deben estar acorde al tipo de investigación que se va a realizar.
- Los investigadores involucrados deben estar capacitados, así como tener la comprensión de todos los pasos tomados en la investigación.

4.3. Diseño del proceso

Este trabajo propone un proceso alineado con los estándares internacionales como son: ISO/IEC 27037 (2012) [13], RFC 3227 [14] y UNE 71505 [15] enfocado a dispositivos móviles. También toma en cuenta guías como: guía forense en teléfonos celulares de Instituto Nacional de Estándares de Tecnología (NIST) [91] y la guía de mejores prácticas para análisis forense en teléfonos

móviles del Grupo de Trabajo Científico sobre Evidencia Digital (SWGDE) [92]. Finalmente, el proceso toma en cuenta todos los estándares, normas, regulaciones y leyes existentes que se mencionaron en el capítulo 2 y da un enfoque de cómo desarrollar una investigación forense en dispositivos móviles.

Los pasos que describen este proceso son: i) identificación y preservación, ii) adquisición, iii) análisis, y iv) documentación. En la Figura 4.1, se observa el proceso descrito anteriormente junto con las entradas y salidas de cada fase la cual ha sido ilustrada utilizando SPEM 2.0 [93].

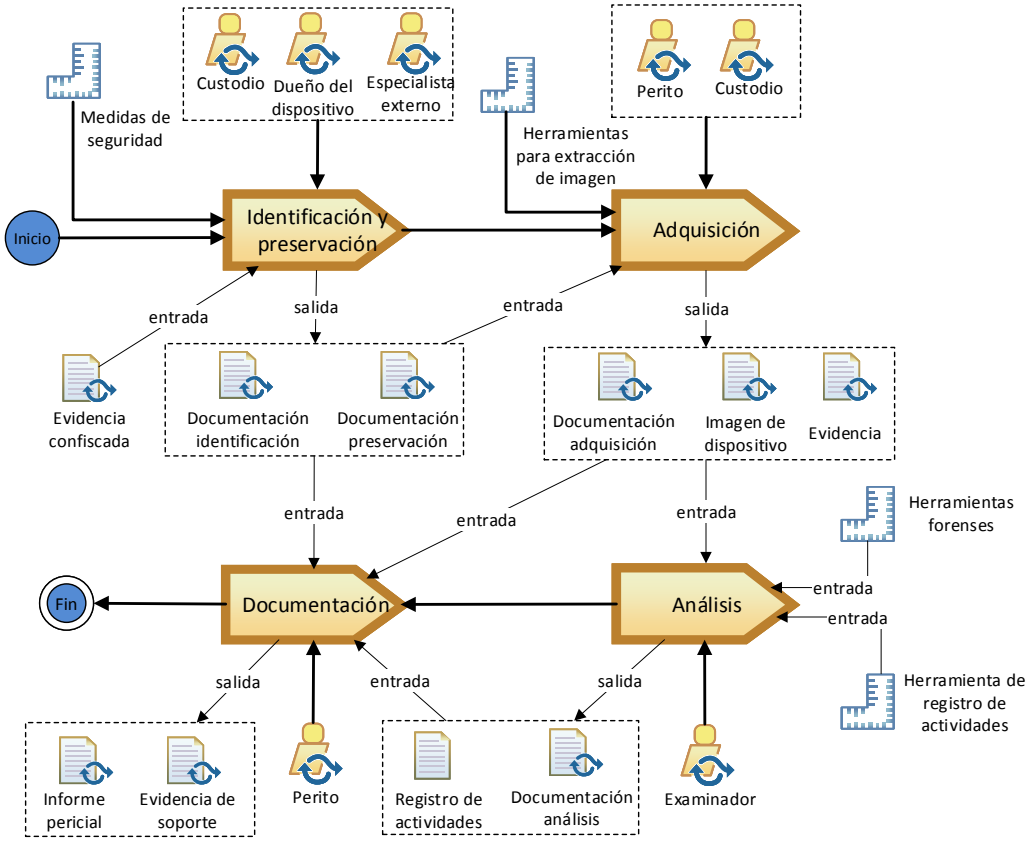


Figura 4.1: Fases del proceso

Las buenas prácticas y el seguimiento de un proceso forense garantizan y dan seguridad a la investigación. Gracias a ésto se evitan errores durante el peritaje y posteriormente sirve como una herramienta de soporte para que el juez tome una decisión adecuada, también ayuda a interpretar la información mediante informes claros y sin entrar en detalles técnicos. En las siguientes sub-secciones se describe cada una de las fases y tareas correspondientes a la

metodología.

4.4. Fase de identificación y preservación

En la primera fase se identifica el tipo de incidente que se va a tratar y las características del dispositivo, mientras se verifica la integridad de la evidencia (CdC) involucrada en su estado inédito.

En la Figura 4.2 se propone un diagrama de flujo donde se muestra las principales actividades para la fase de identificación y preservación.

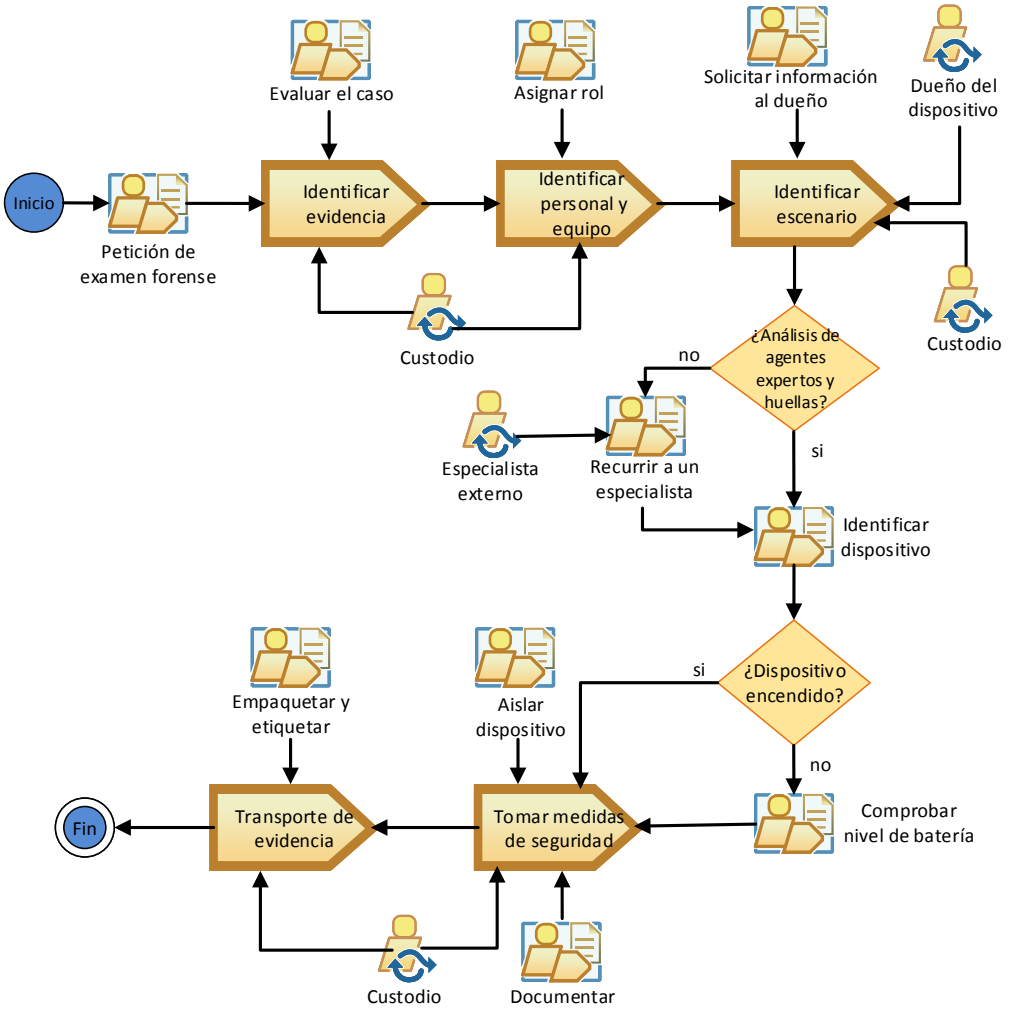


Figura 4.2: Diagrama de flujo de la fase de identificación y preservación

4.4.1. Identificación de la evidencia

Los dispositivos móviles deben tener un tratamiento adecuado, ya que la evidencia puede verse comprometida por un manejo incorrecto y de esta forma ser invalidada.

Identificar el problema

1. El primer paso para empezar la investigación será una solicitud de examen forense para

el objeto que está involucrado. Ahora se puede decir que una solicitud de examen forense es un documento formal, notariado o una petición de un juez a través del consejo de la judicatura, el cual da información de la institución o persona solicitante, el objeto de la pericia, el o los dispositivo(s) y las firmas pertinentes. Todo esto se realiza siguiendo las leyes vigentes.
2. Se debe realizar el proceso siguiendo las leyes vigentes caso contrario el investigador puede ser sancionado por los Artículos 232 y 234 según el Código Orgánico Integral Penal (COIP).
3. Desarrollar estrategias según en caso de estudio, determinar el equipo y el personal para la investigación.

4.4.2. Identificación del personal y equipo

1. El personal que interviene en la investigación debe ser registrado según la tarea que va a desarrollar. El registro debe contener el nombre de cada miembro del personal, la actividad que va a realizar y si se encuentra en la escena y/o laboratorio de investigación.
2. Cada miembro del personal tendrá un rol específico como por ejemplo investigadores o peritos, custodios y examinadores. Este paso es importante, ya que se restringe el acceso a personas externas.

4.4.3. Identificación del escenario

En la fase de asegurar la escena es donde se restringe el acceso para que ningún objeto o persona puedan alterar la escena y la investigación tal como dice “Principio de intercambio de Locard” [52]. Ahora todos los investigadores que están involucrados en el proceso deben garantizar que las acciones sean seguras y verídicas, para ello se debe tomar las siguientes normas y protocolos:

1. Identificar la escena para establecer un perímetro y salvaguardar la investigación; de esta manera restringir el acceso a personas o equipos informales que puedan alterar la escena.
2. Solicitar información al dueño del dispositivo.
3. Restringir el uso de dispositivos inalámbricos dentro del perímetro.
4. Documentar la fecha y hora en forma de fotografías y videos.
5. Documentar todo el proceso de investigación en línea, de igual manera con imágenes y videos.
6. Todos los objetos en la escena deben ser manipulados con guantes de látex, así no se altera de ninguna manera la evidencia. Ésto en el caso de que se trate de la recolección del dispositivo, donde se haya desarrollado algún delito penal (homicidios, violación, robo,

entre otros agravantes), de ser el caso hay que precautelar las evidencias transferidas a los dispositivos.

7. La evidencia que abarca los dispositivos móviles, cables, adaptadores, unidades extraíbles para realizar una copia o imagen forense.
8. Los dispositivos tienen códigos para eliminar información luego de intentar varios accesos fallidos, debido a esto se restringe al propietario o persona informal la manipulación del dispositivo. Existe maneras de destruir información de manera remota por lo que se debe asegurar y aislar el dispositivo móvil.
9. La evidencia puede estar contaminada por agentes externos como líquidos, tierra, etc., en dichos casos se recomienda consultar a un especialista para la limpieza de los dispositivos.
10. En dispositivos dañados o parcialmente destruidos, se trata de salvar los componentes y extraer información.

4.4.4. Medidas de seguridad

1. Cada elemento incautado debe ser protegido y almacenado, la manera más segura es etiquetarlo con toda la información (fecha, hora, persona responsable, etc.)
2. Si el dispositivo está encendido se procede a: verificar el porcentaje de batería, fotografiar lo que contiene en la pantalla.
3. Al ser incautado, el dispositivo móvil, debe ser aislado; la técnica que debe aplicarse es poner el teléfono en modo avión. También debe desconectarse de las redes: Wi-Fi, Bluetooth, infrarrojo, etc.
4. El dispositivo debe colocarse en jaulas de Faraday [6] que son bolsas o cajas recubiertas de una malla metálica que aísla las señales inalámbricas, así el dispositivo preservará la evidencia digital evitando accesos remotos no autorizados.

4.4.5. Transporte de evidencia

1. Cada evidencia se coloca en un paquete, éste debe ser sellado, con la documentación. El paquete no debe ser abierto hasta llegar al laboratorio o sitio donde se realizará el análisis.
2. El transporte debe ser seguro, el ambiente debe ser regulado, así como evitar golpes y agentes externos que perturben el estado del paquete.

4.5. Fase de adquisición de la evidencia

Hoy en día los dispositivos móviles poseen gran capacidad de almacenamiento y la evidencia que contiene en ellos puede eliminarse o modificarse en general. Se presenta las medidas que se

deben tomar cuando el paquete con la evidencia llega al laboratorio o al lugar donde se realiza el análisis. En la fase de adquisición se debe tener una elevada precaución para no modificar la evidencia, en esta fase se realiza una imagen forense o *backup* bit a bit de la memoria del dispositivo.

En la Figura 4.3 se propone un diagrama de flujo donde se muestra las principales actividades para la fase de adquisición. También conocer después de que actividad se debe documentar, así no omitir ninguna actividad en el registro de actividades.

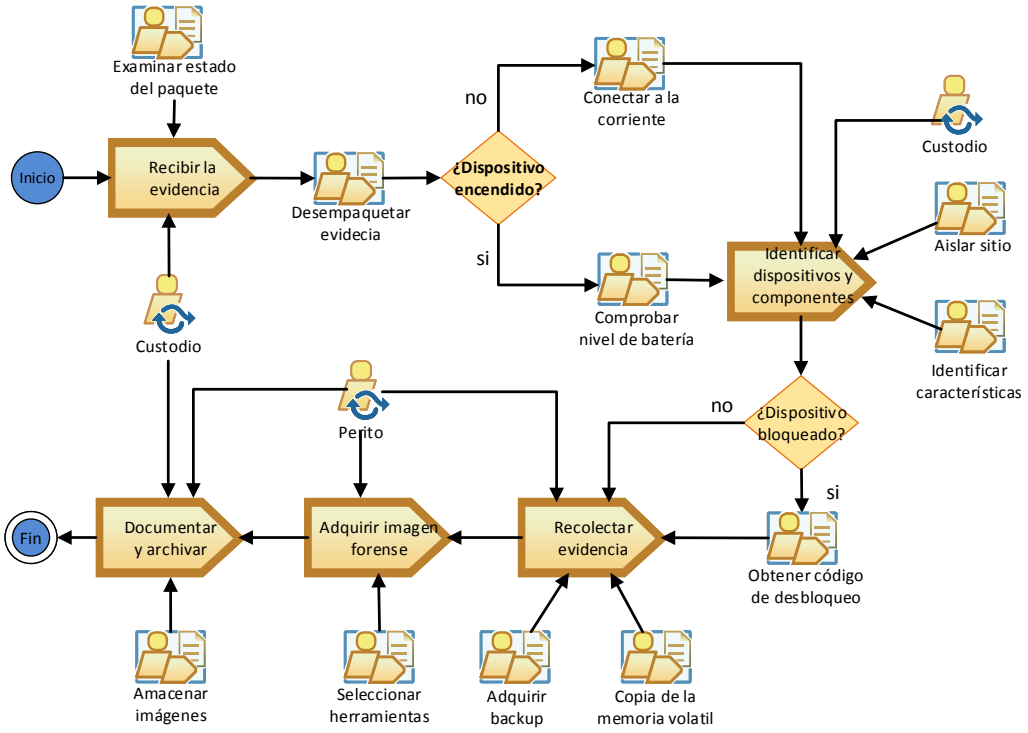


Figura 4.3: Diagrama de flujo de la fase de adquisición.

4.5.1. Recepción de la evidencia

1. El laboratorio debe estar equipado.
2. La fecha, la hora y el responsable cuando llega el paquete deben ser registrados, éste paso es conocido como la "cadena de custodia".
3. Examinar si el paquete está en buenas condiciones.
4. Si acaso hubo alguna alteración, pérdida o manipulación de la evidencia esta debe ser registrada, también se debe verificar los datos de la fase anterior.

4.5.2. Identificación dispositivos y componentes

1. El primer paso es aislar el sitio de investigación de cualquier red inalámbrica. Una técnica para realizar este paso es mediante inhibidores de señal.
2. Los objetos deben ser siempre manipulados con guantes de látex.
3. Identificar todas las características del dispositivo (modelo, marca, periféricos, cables, accesorios, etc.)
4. Se debe verificar el nivel de batería del dispositivo
5. Se registra los pasos anteriores mediante fotografías especialmente la pantalla del dispositivo la cual contiene el nivel de batería.

4.5.3. Recolección de evidencia y copia de seguridad

1. Identificar la evidencia.
2. Obtener una copia de la memoria no volátil. Para ejecutar el volcado de memoria se utiliza dispositivos o *software* forenses especiales para esta tarea.
3. Se comprueba si el dispositivo está bloqueado ya sea: i) modo básico (desplazar la pantalla); ii) código de 4 dígitos (PIN); iii) contraseña de cuatro dígitos; y iv) patrón con mínimo cuatro puntos.
4. Adquirir un *backup* de la información del dispositivo. Se comienza conectando el móvil al computador mediante un cable USB, para instalar todos los *drivers* que son necesarios para el dispositivo.
5. Se adquiere una copia de seguridad (*backup*) del dispositivo, de igual manera que en la memoria no volátil se puede utilizar un dispositivo o *software*.

Los riesgos en este paso son: la mala manipulación del dispositivo móvil e inexperiencia del manejo de las herramientas de *backup* lo que resulta en alteración de la evidencia.

4.5.4. Imagen forense

1. Conocer donde está la información que se va analizar.
2. Seleccionar la herramienta para la extracción y adquisición de la imagen del dispositivo.
3. Extraer una copia de todo el dispositivo, a menos que exista una petición de extracción de información específica.
4. Comprobar *hash* de la copia de la información que se haya realizado y verificar que no esté alterada.

El riesgo más notable en esta fase es no conseguir una copia exacta de toda la información del

dispositivo.

4.5.5. Documentación y archivar

1. Se debe documentar todo el procedimiento en un registro histórico.
2. Las copias de seguridad y la imagen forense deben ser almacenadas en una carpeta o dispositivo exclusivamente para la investigación.

4.6. Fase de análisis

Esta fase es un desarrollo técnico, donde con la copia de seguridad de el/los dispositivo(s) y con las herramientas necesarias, se comienza a hallar las pruebas en la investigación. El conjunto de datos extraídos debe ser analizado según caso de estudio.

La potencial evidencia que se podría encontrar son fotos, correos electrónicos, historial de navegador, mensajes, llamadas, entre otras actividades que el usuarios realiza en su dispositivo. En la Figura 4.4 se propone un diagrama de flujo donde se muestran las principales actividades para la fase de análisis.

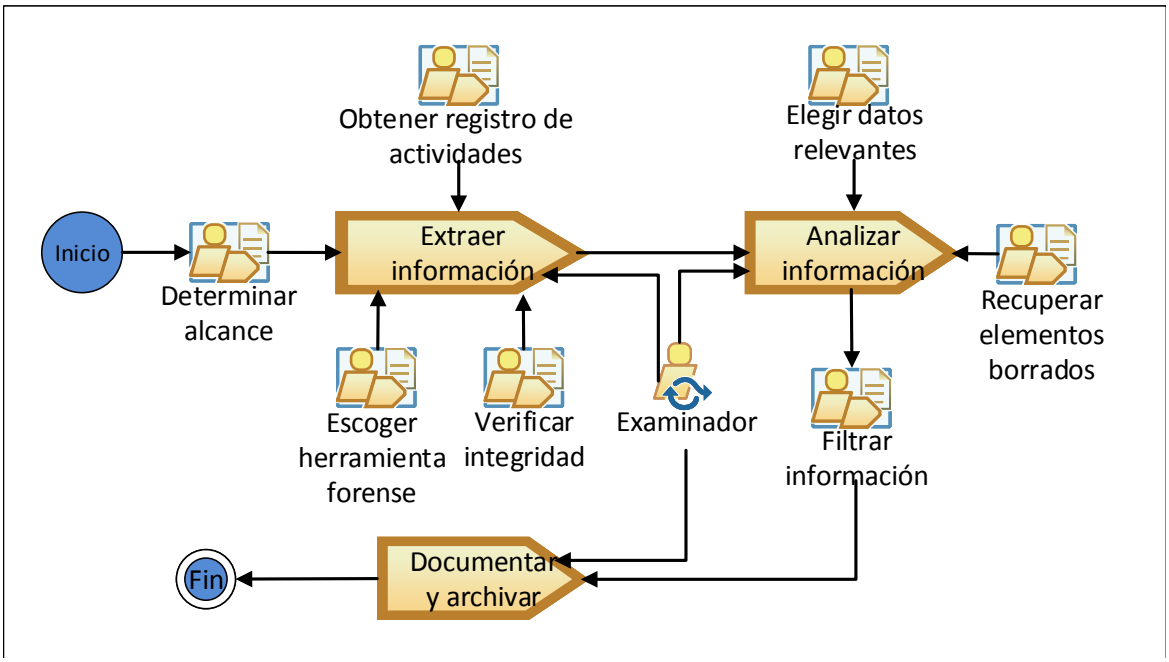


Figura 4.4: Diagrama de flujo de la fase de análisis.

4.6.1. Alcance

Cada caso de estudio es diferente y debe evaluarse para determinar el alcance de la investigación. Las interrogantes que se generan pueden ser: ¿cuál es el propósito para recolectar los datos?, ¿qué tipos de datos se pueden adquirir?, ¿cuán importante es la obtención de datos?, ¿qué debe ser analizado?, ¿qué puede ser analizado?, etc.

4.6.2. Extracción de la información

1. Verificar el *hash* de la imagen que se extrajo en la fase anterior, esto revela la integridad de la información.
2. Para no alterar la información se realiza un respaldo de la imagen original, se almacena en una ruta especifica.
3. Escoger las herramientas necesarias para la extracción de los registros y datos. Las herramientas que van acorde a este proceso son: Andriller, Oxygen Forensic, MOBILEedit, Autopsy, Bulk extractor y Kali Linux.
4. Cada herramienta genera un informe en diferentes formatos, los cuales mediante RegistroActividades se compactan en un informe general.

El riesgo para este paso es no capturar la información necesaria o incluso pérdida de ésta, la cual sería de interés para el informe final. En la Figura 4.5 se muestra el flujo de la fase de extracción de la evidencia digital, en cada tarea el único actor designado es el analista.

4.6.3. Análisis

1. Elegir los datos más relevantes para la investigación, es decir, que la información sea pertinente para el caso.
2. Rescatar los elementos borrados, teniendo en cuenta que éstos puedan recuperarse.
3. Se establece una línea de tiempo con las actividades del dispositivo realizadas por el usuario.
4. Filtrar los datos en un rango de tiempo para obtener información específica o importante.

4.6.4. Documentación y archivar

1. Se documenta todo el proceso y hallazgos descubiertos.
2. Se documentan todas actividades realizadas en cada fase del proceso mediante un registro histórico.

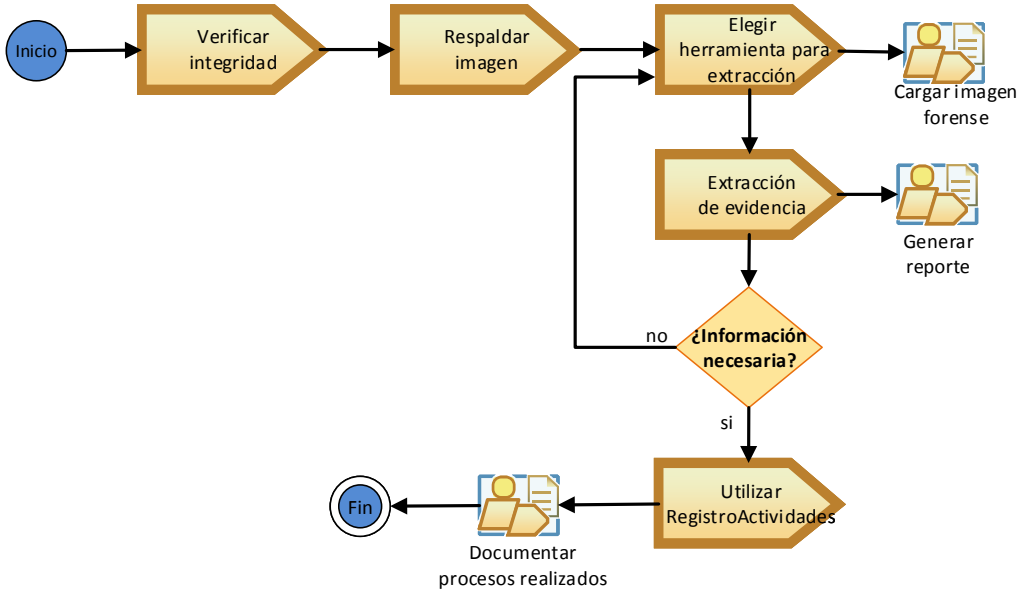


Figura 4.5: Diagrama de flujo de la fase de extracción.

El riesgo más importante sería el de no documentar alguna prueba importante o en otro caso de una incorrecta documentación de cada actividad realizada por el encargado. Ésto conlleva a la exclusión de evidencia probatoria.

4.7. Informe

En esta fase se presentan los informes finales, es decir, se documenta de manera formal todos los hallazgos y resultados en forma resumida y clara.

Informe pericial

Se describe las tareas que se ejecutaron en el proceso, con los dispositivos forenses, las herramientas, en el dispositivo móvil, etc. En otras palabras se sintetiza todas las tres fases anteriores en un informe final. En la Figura 4.6, se describen las tareas y sugerencias a considerar durante ésta fase.

El registro debe contener pruebas fotográficas, así como contenido producido por las herramientas de *hardware* o *software* que se utilizaron a lo largo de la investigación. El informe pericial final según el Consejo de la Judicatura [94] debe abarcar los siguientes puntos:

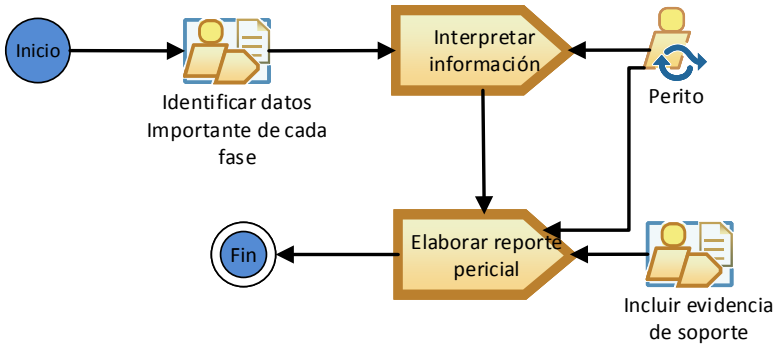


Figura 4.6: Diagrama de flujo de la fase de documentación.

1. Datos generales del juicio, o proceso de indagación previa
2. Antecedentes
   - Datos generales
   - Descripción del caso de estudio
   - Alcance
   - Objeto de la pericia
   - Personas involucradas
   - Sitio del suceso
3. Parte de consideraciones técnicas o metodología a aplicarse
4. Conclusiones
5. Inclusión de documentos de respaldo, anexos, o explicación del criterio técnico
   - Pruebas visuales
   - Herramientas (*hardware* o *software*)
   - Sustento técnico o científico
   - Reseña detallada del dispositivo
   - Resultados descubiertos
   - Observaciones
6. Información adicional
   - Datos generales
   - Conceptos y definiciones
7. Declaración juramentada
8. Firma y rúbrica

Capítulo 5

Herramienta: Registro de actividades

En este capítulo, se desarrolla la herramienta que será capaz de generar una lista con las actividades que el usuario realizó en su dispositivo móvil en un tiempo determinado. En la sección 5.1 se da una breve introducción al capítulo, en la sección 5.2 se propone el diseño para el desarrollo de la herramienta, la sección 5.3 explica las principales características del programa. Finalmente, la sección 5.4 se presenta los problemas y las soluciones que tuvo el desarrollo de la herramienta.

5.1. Introducción

La herramienta desarrollada está destinada para los reportes generados por los paquetes de *software* forenses los cuales extraen información digital de teléfonos inteligentes, y se implementó en el lenguaje de programación Python [81]. La herramienta recopila información de diferentes *software* dedicados a la extracción y análisis forense en dispositivos móviles que cuentan con el SO Android, a partir de toda esta información es posible obtener las actividades que el usuario desarrolló en su dispositivo. Por lo tanto, la finalidad es mostrar en un documento varios datos obtenidos y otorgar a los investigadores un medio visual de las acciones realizadas en dicho dispositivo. A continuación se determina el funcionamiento general.

5.2. Diseño

Antes de manejar cada archivo es necesario conocer su estructura, como están distribuidos, que información contiene, la ruta donde están almacenados, entre otros aspectos. Según la UNE 71505 [15], es importante conocer estos datos debido a que el programa que se desarrolla no debe alterar dichos archivos considerados como evidencia. En la sección 5.2.1 se describen la composición de los reportes entregados por el paquete de *software* forense.

5.2.1. Estructura de archivos

De acuerdo con los objetivos planteados, es necesario escoger el paquete de *software* (herramientas forenses) adecuados para la extracción de evidencia digital en un dispositivo móvil con SO Android. En el capítulo 2 del trabajo, se explica las herramientas que van a ser utilizadas, éstas proporcionan un reporte en diferentes formatos que contienen información de los datos extraídos del dispositivo; como se observa en la Tabla 5.1 se muestra los diferentes formatos de reporte que genera cada herramienta. Andriller, MOBILedit y Oxygen Forensic fueron instalados en Windows por su mejor rendimiento en este SO, mientras que, Kali Linux con sus herramientas internas en Linux se escoge el formato .xlsx para las tres primeras opciones y texto para la última herramienta. Cabe resaltar que, dentro de Kali Linux está incorporado Autopsy y Bulk_extractor como herramientas principales, mientras que, binwalk, Chkootkit, foremost, galleta y volatility como sub-herramientas en Kali Linux.

Cada reporte generado posee información del dispositivo móvil como los que se presentan en la Tabla 5.2 que a su vez proporcionan información como: nombre del dato, etiqueta, en el caso de navegación web la URL, directorio, nombre de carpeta que la contiene, última visita, fecha que se accedió, fecha en la que se modificó, tamaño, fecha que se creó, tipo de archivo, descripción, como

Tabla 5.1: Formato de los reportes

Herramienta	Tipo de archivo
Andriller	Excel (.xlsx), HTML
MOBILedit	Excel (.xlsx), HTML, PDF
Oxygen Forensic	Excel (.xlsx), XML, HTML, RTF, PDF
Kali Linux	Texto (text)

principales datos. Mientras que, para el caso de llamadas, mensajes, calendario y contraseñas se proporciona: nombre, fecha en la que se realizó la actividad, duración del mismo y una descripción breve.

Tabla 5.2: Información en un reporte

Información
Información del caso
Datos del investigador
Características del dispositivo
Fecha en la que se realiza la extracción
Calendario (eventos programados)
Wi-fi (contraseñas)
Historial de navegación web (Chrome)
Búsqueda en el historial de navegación
Multimedia (foto, video, audio)
Aplicaciones (instaladas, eliminadas)
Uso de aplicaciones
Historial de descargas
Cookies
Almacenamiento
Lista de llamadas
Mensajes SMS
Archivos eliminados
Memoria externa SD

Como se menciona a lo largo del capítulo, cada *software* forense devuelve un reporte. Ahora, dependiendo de la herramienta forense puede devolver no solo un reporte; sino un conjunto de reportes cada uno con las características de la Tabla 5.2. En las Figuras 5.2 y 5.1 mediante un ejemplo se recolectaron 10 reportes con el paquete de *software* en Windows mientras que, en Linux se obtuvieron 7 reportes. Ésto varía dependiendo de la cantidad de información que contenga el dispositivo móvil.

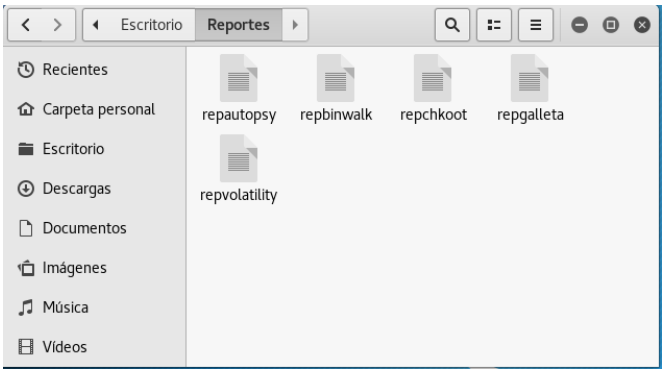


Figura 5.1: Carpeta de reportes de herramientas en Linux.

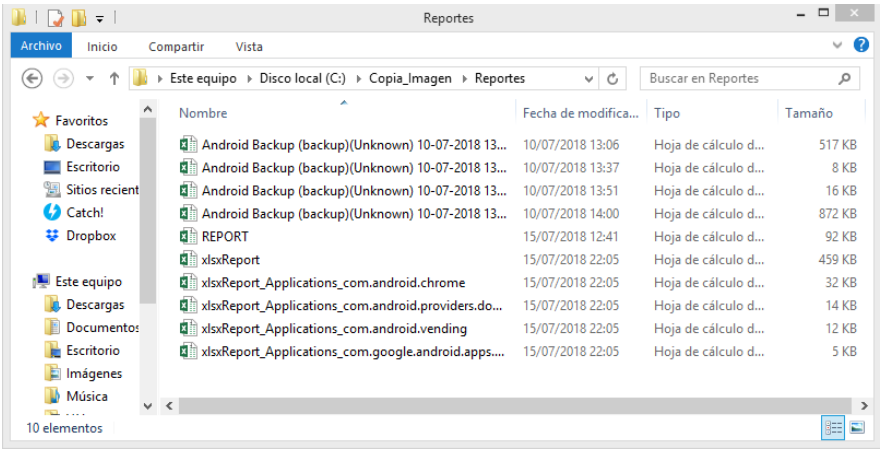


Figura 5.2: Carpeta de reportes de herramientas en Windows.

5.2.2. Lenguaje de programación

El lenguaje de programación que se emplea es Python [81], cuya filosofía es una sintaxis limpia y código legible, además de ser un lenguaje sencillo y fácil de utilizar. Python es de código abierto y libre, lo que permite crear aplicaciones e involucrase en el desarrollo. Por otra parte, Python está presente en varios servicios que se utilizan cotidianamente y en empresas de prestigio como Google, Youtube o Facebook. Finalmente, este lenguaje de programación está disponible en varias plataformas como: Windows, Mac OS y UNIX/Linux [95] .

Ésto demuestra que Python es una opción viable que existe en el mercado. En el área forense de dispositivos móviles existe una desigualdad entre *software* comerciales y de código abierto debido a que, la mayoría son de tipo comercial. Según Limodio et al.,en [28] mensionan que las herramientas forenses de código abierto permiten al perito, juez o la parte afectada verificar

que la evidencia no haya sido manipulada, tienen errores o fallas. Por último, se debe tener en cuenta que el *software* es solo una herramienta y el éxito de su respuesta depende del profesional que la opera.

En el capítulo 2 se revisó varias herramientas forenses tanto para SO Windows y Linux. Para el caso del paquete de *software* forense en Linux cada uno de ellos trabaja mediante comando por consola, ésto no disminuye su eficiencia y mucho menos su potencial. Por este motivo se decide trabajar de la misma manera en Python; es decir, de una manera intuitiva y sencilla para el usuario.

5.2.3. Funcionamiento

Se han agrupado las actividades en cuatro procesos principales que son: identificación, recolección, análisis y preservación. En cada una de éstas existen procesos y tareas que deben ser realizadas. La Figura 5.3, muestra las actividades y procesos principales que ejecuta la herramienta planteada.

El programa permite obtener los datos de reportes generados por los distintos *software* forenses; se deben tener todos los reportes en una carpeta para que posteriormente la aplicación pueda leerlos. La herramienta desarrollada cumple con lo siguiente:

- Detectar y contar la cantidad de archivos según su tipo.
- Determinar el número de hojas y filas en los archivos excel mientras que, para los archivos texto determinar la cantidad de lineas, ésto se realiza para indicar hasta donde debe leer cada archivo.
- Obtener la columna que contenga la fecha y hora de la actividad para el caso de archivos excel.
- Comparar la fecha ingresada con las fechas de la columna en excel, para el caso de los archivos texto comprar con el texto fila por fila.
- Guardar los datos filtrados.
- Unir los datos en un solo archivo.
- Ordenar de forma descendente para así obtener las actividad más recientes a las más antiguas.
- Eliminar los datos repetidos mediante la etiqueta que contiene cada uno.
- Asignar un código a cada actividad.
- Guardar el registro.
- Filtrar datos mediante el ingreso de los códigos.

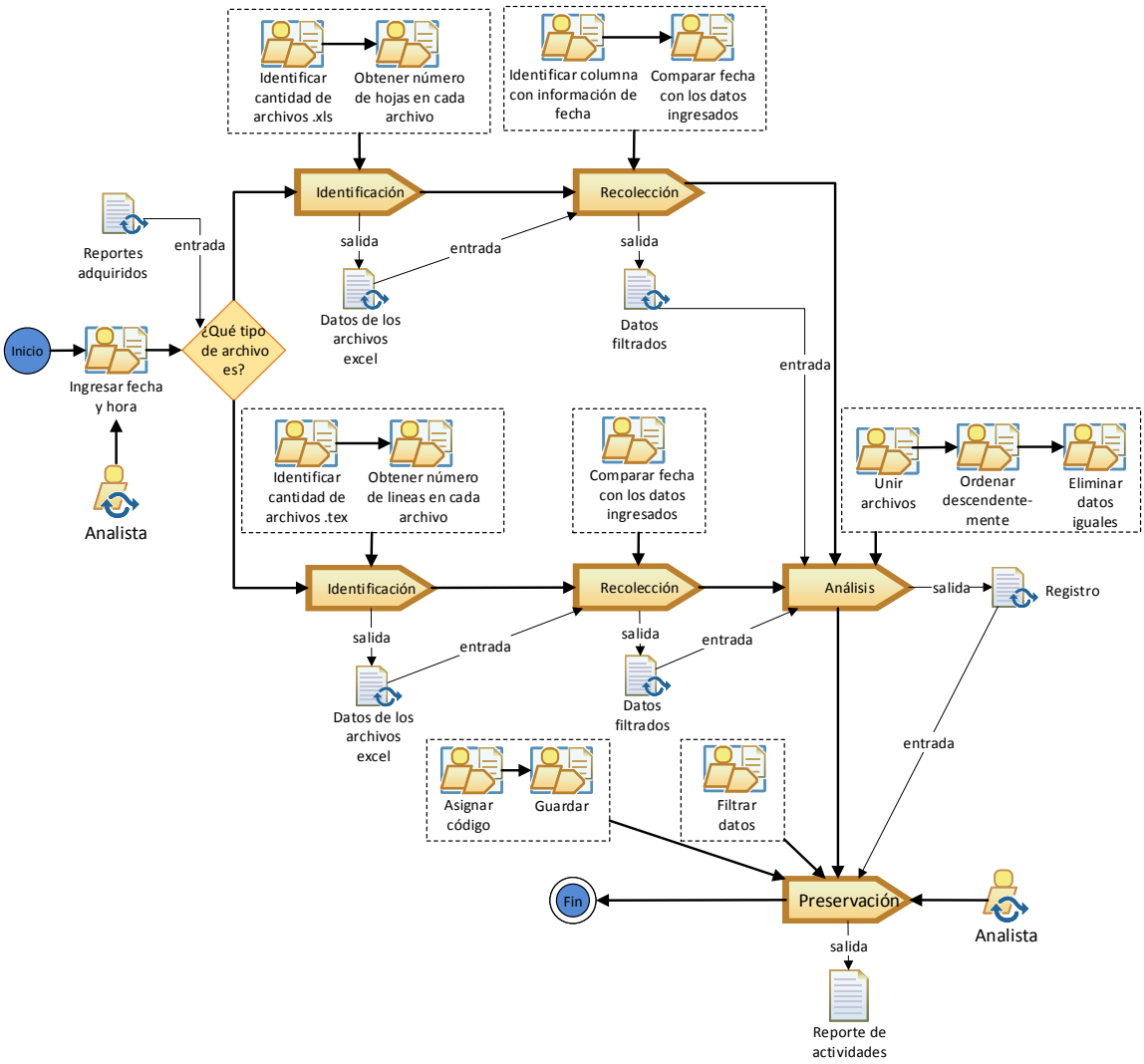


Figura 5.3: Tareas y procesos de la herramienta planteada.

5.3. Implementación

La herramienta ha sido desarrollada en Python, en el SO Linux. En esta sección se describe la implementación de las tareas y procesos señalados en la Figura 5.3. Para ejecutar el programa lo primero se debe realizar es abrir la terminal e ingresar la siguiente linea:

```
python RegistroActividades.py
```

Ésta línea llama al programa principal como se observa en la Figura 5.4, inmediatamente se ingresan y validan los datos requeridos para la investigación (fecha y/u hora). Se exige que la fecha u hora ingresadas sean en el formato dd/mm/aaaa para la fecha y para la hora hh:mm:ss, caso contrario se muestra un mensaje de validación como se observa en la Figura 5.5.

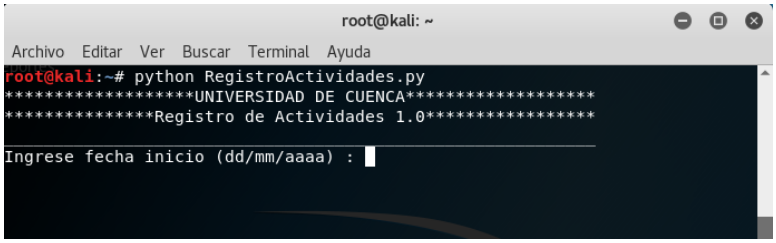


Figura 5.4: Presentación de la herramienta para el registro de actividades.

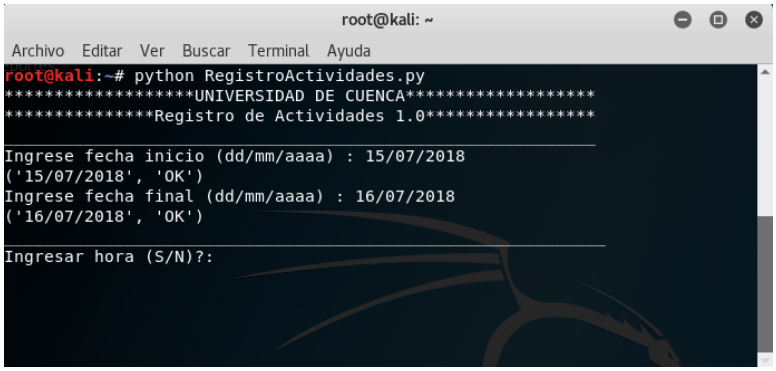


Figura 5.5: Validación de datos ingresados.

5.3.1. Identificación

En la identificación, como se ha ido mencionando a lo largo del capítulo se va a trabajar con dos tipos de archivos, cabe resaltar que dichos archivos deben estar en una carpeta llamada Reporte. El primer paso es determinar la cantidad de archivos que contiene la carpeta según su tipo, ésto se realiza ya que posteriormente se dará un procesamiento diferente a cada uno.

Para el caso de archivos excel que son obtenidos del paquete de *software* forense en Windows se identifica el número de archivos, dentro de cada archivo la cantidad de hojas y su vez el número de filas y columnas. Estos datos serán de utilidad para el desarrollo del programa, debido a que, es necesario recorrer cada uno de los archivos recolectando información y sin obviar ninguna hoja, fila o columna. En el caso de las herramientas en Linux, de igual manera se identifica el número de archivos con la diferencia que dentro de cada uno se obtendrá la cantidad de lineas.

5.3.2. Recolección

Una vez identificados los primeros datos, se procede a recolectar la evidencia almacenada en los reportes. Para el caso de archivos excel como se explicó en la sección 5.2.1, cada hoja en este tipo de archivos contiene información del dispositivo, dentro de estas hojas existe una columna la cual contiene la fecha y hora que se realizó la actividad. Ya identificada dicha columna el programa empieza a comparar las fechas, al encontrar una coincidencia se guarda toda la fila en un archivo texto. Por otro lado, para el caso de los archivos texto se compara la fecha ingresada con cada fila, de igual manera se guarda en un archivo texto.

5.3.3. Análisis

Ya obtenidos los datos filtrados se procede a unir los reportes en un solo archivo, cabe resaltar que ningún procedimiento debe realizar tareas de escritura ya que ésto alteraría la evidencia. Se emplea un algoritmo para ordenar según la fecha y hora que se determinó anteriormente; de la actividad más reciente a la más antigua. Por último, se elimina los datos con etiqueta y fecha igual; ésto para eliminar información repetida que no es de ayuda para la investigación.

5.3.4. Preservación

Finalmente, una vez obtenido todo el registro limpio de información repetida se asigna un código "arxxx" a cada actividad y se lo guarda en un archivo texto llamado ReporteFinal. Por otra parte, se da una opción que es filtrar información; ésto se realiza para obtener la información que el investigador considere relevante para el caso. En la parte inferior de la Figura 5.6 a manera de ejemplo se muestra la opción de filtro.

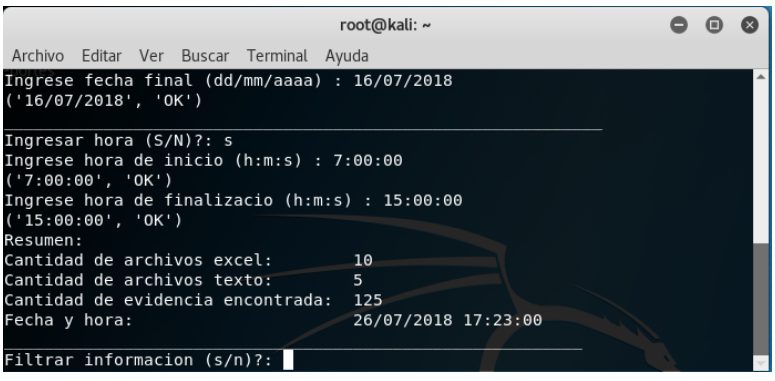


Figura 5.6: Herramienta para el registro de actividades.

Como proceso adicional, el programa imprime un resumen con la cantidad de archivos de cada tipo, la cantidad de actividades recolectadas en el rango de tiempo establecido, la fecha y hora que se obtuvo el informe final e informe filtrado. Por último, en el caso que el código ingresado no existe o está incorrecto se imprime en el resumen. Siguiendo el mismo ejemplo en la Figura 5.7 se imprime el resumen tanto del registro original como el registro filtrado.

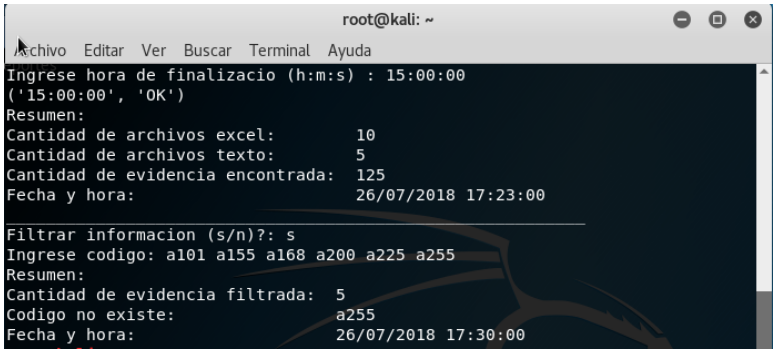


Figura 5.7: Resumen del registro de actividades.

5.4. Resultados

A partir de varias pruebas realizadas en distintas marcas de dispositivos móviles con SO Android, se puede afirmar que la herramienta de registro de actividades es estable y cumple con los parámetros propuestos. Existen algunos errores al mostrar la lista ya que se duplica la información de algunas actividades, pero es debido a que dos o más herramientas forenses registraron la misma actividad; sin embargo, es posible omitir esos pequeños errores con el proceso de filtrado de información ya que no representan un mayor problema para los fines posteriores de la investigación.

La principal ventaja que se halló al utilizar ésta herramienta es el ahorro de tiempo y recursos, debido a que cada *software* instalado devuelve grandes volúmenes de información que deben ser analizados paso a paso por el investigador encargado, además, es necesario más de un *software* para obtener toda la información que se requiere para el caso.

Finalmente, en la implementación de herramienta se tuvo especial cuidado en el manejo de la evidencia, ya que ésta no debe ser alterada ni manipulada de forma incorrecta. Al ser alterada de alguna forma ésta no será válida para la investigación y para casos judiciales.

Capítulo 6

Prueba de Concepto

En este capítulo se cumple el último objetivo planteado en este trabajo, éste es aplicar el proceso y la herramienta mediante una prueba de concepto. En la sección 6.1 se da una introducción del caso que se plantea, la sección 6.2 describe el escenario para el caso de prueba, la sección 6.3 establece todos los parámetros necesarios como es el personal, tipo de dispositivo y manejo de la evidencia, la sección 6.4 proporciona las herramientas necesarias para la adquisición de la evidencia, la sección 6.5 plantea la forma de extraer y análisis de la evidencia en forma de bitácora, finalmente, en la sección 6.6 se documenta todos los pasos realizados a lo largo de la investigación y finalmente, en la sección 6.7 se detallan los resultados más importantes de la prueba de concepto.

6.1. Introducción

En este capítulo se procede con la implementación del proceso y herramienta , se ha propuesto un escenario que permite demostrar la eficiencia de la propuesta de este trabajo. Para comprobar la validez de la guía, se ha procedido a realizar el análisis forense a un dispositivo Android. El dispositivo que se analiza es un celular de la marca Samsung, modelo J1 Ace con SO 4.4.4.

La presente prueba de concepto se realiza para analizar la información digital generada por un dispositivo móvil y proporcionar un informe pericial. Además, el objetivo de esta prueba es determinar el correcto uso del proceso metodológico para el análisis de la evidencia que se plantea en el capítulo 4, así como emplear la herramienta RegistroActividades propuesto en el capítulo 5.

6.2. Descripción del escenario

El escenario propuesto para este caso es de ámbito universitario, debido a que en la actualidad una de las preocupaciones de las instituciones educativas es la utilización de medios electrónicos no solo como ayuda para el proceso de aprendizaje; sino que los estudiantes están haciendo uso de la tecnología, específicamente dispositivos móviles en temas relacionados con copia en evaluaciones académicas (exámenes). El contexto que se desarrolla el escenario es un examen realizado a los estudiantes de octavo nivel de la asignatura de Organización y Evaluación de Proyectos de la facultad de Ingeniería de la Universidad XYZ, el examen se desenvolvió en el horario de 11h00 a 13h00 el 9 de julio de 2018.

Antes de iniciar el examen el profesor encargado expuso que, no está permitido el uso de ningún tipo de ayuda ya sea apuntes, libros, calculadora, computador y/o celular; de ser el caso se retirará el examen y se procede informar el hecho a la doctora abogada de la facultad para que proceda a efectuar las medidas pertinentes en el caso de acuerdo al reglamento interno ante fraudes académicos por presunción de copia. Durante el transcurso del examen el docente notó que un estudiante realizó un movimiento sospechoso, al ver ésto el docente se acercó al estudiante y verificó que poseía un dispositivo móvil escondido en donde se estaba presuntamente cometiendo la copia, por lo que se le pidió al estudiante entregar el examen y retirarse.

Ante este contratiempo el estudiante afirma que no realizó ningún intento de copia, si no que solamente saco su teléfono para ver la hora y verificar el tiempo que le quedaba hasta la finalización del examen.

El docente solicita incautar el dispositivo para determinar las actividades que realizó durante el

examen y de este modo verificar si están relacionadas con el tema de la asignatura. Para dicho fin, se solicita desarrollar un análisis forense al dispositivo del estudiante, el informe pericial será utilizado por el consejo de facultad para determinar las acciones a tomar con el estudiante.

6.3. Identificación y preservación

Esta fase ocurre antes de que empiece la investigación como tal. Se debe entender la naturaleza de la infracción o delito, las causas que la provocaron, las personas involucradas y el escenario donde se desenvuelve el incidente.

Ahora, ya conocidos todos los datos necesarios para empezar la investigación el siguiente paso es la identificación y definición del caso, así como el alcance y los objetivos. Es importante determinar claramente el objetivo principal y la justificación por la cual se lleva a cabo la investigación. Luego de tener bien definido estos puntos se procede a realizar la solicitud de examen forense (Apéndice A).

6.3.1. Identificar problema

Objetivos

El objetivo principal de esta investigación es obtener la mayor cantidad de información alojada en el dispositivo móvil el cual ha sido identificado como la herramienta para plagio perteneciente al estudiante Juan Perez de manera menos intrusiva. Se extraen las actividades que se desarrollaron en el dispositivo el día del examen 9 de julio de 2018 en el horario de 11h00 a 13h00.

Justificación

Al realizar un examen a los estudiantes de octavo nivel de la asignatura de Organización y Evaluación de Proyectos de la facultad de Ingeniería de la Universidad XYZ, el docente se percata de que un estudiante realizó un intento de copia, por lo que se verificó y se descubrió que poseía un dispositivo móvil escondido, por lo que se le pidió al estudiante entregar el examen y retirarse.

El docente ha solicitado que se realice una investigación de las actividades que realiza el estudiante con dicho teléfono, debido a la sospecha de una posible copia durante la evaluación académica. En el Apéndice A se detalla la solicitud de examen forense.

6.3.2. Identificar personal y escenario

En los pasos anteriores se consiguió un perfil sobre el estado inicial del evento, el cual ayudará a guiar las acciones posteriores. Una vez que se decidió a donde va dirigida la investigación, fechas en las que se quiere conseguir los datos y el dispositivo que se va analizar, se procede a identificar al personal encargado en cada una de las fase y asegurar la escena.

Para seguir el proceso del capítulo 4 en la Figura 6.1 se muestra los pasos a seguir. En el cuadro azul se encierra la identificación y en el cuadro rojo la identificación de la escena.

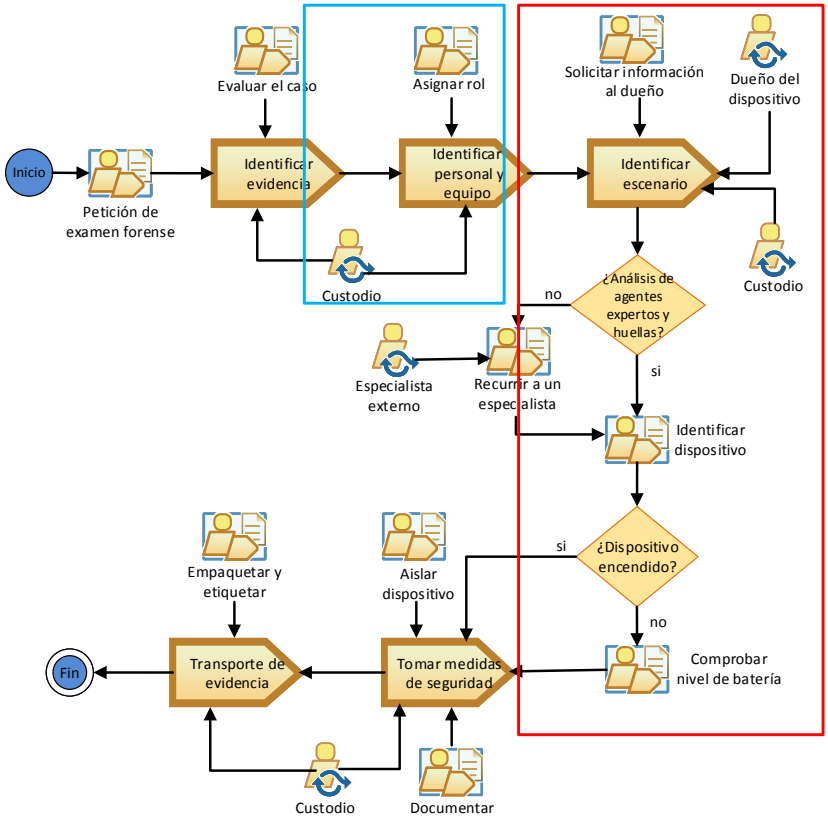


Figura 6.1: Identificar personal y escena.

Personal

En la identificación del personal se debe tener mucho cuidado, ya que éste va a estar involucrado de forma directa, para ésto hay estándares mínimos que deben acatar el personal forense y de

investigación. Tales estándares deben cubrir los conocimientos técnicos y administrativos, así como se debe tener extremo cuidado con la evidencia y profesionalismo en toda la investigación. A cada persona se le asignará una tarea que debe cumplir y toda actividad que se realice debe estar registrada. Para este caso donde se tiene un dispositivo se va a necesitar tres encargados los cuales deben cumplir con el rol de investigador/perito, custodio y examinador/analista.

Escena

Para el aseguramiento de la escena debe existir un protocolo formal, este protocolo se encarga de transferir al personal encargado de la escena y restringir el acceso no autorizado, así como evitar que la evidencia se contamine. En el caso de dispositivos móviles no solo estos son considerados como evidencia sino también sus accesorios (cable USB, cargador, SIM, memoria externa, etc.). Ya que hoy en día los dispositivos móviles pueden ser sincronizados fácilmente por medio de un dispositivo PC es necesario aislar el teléfono de cualquier red inalámbrica (ejm. Wi-Fi, Bluetooth, Inforarrojo). Si es necesario se puede pedir la ayuda de un experto en esta fase, se debe realizar una valoración del equipo.

Por otra parte, es importante establecer entrevistas con el dueño del dispositivo, en este caso un estudiante de la asignatura Organización y evaluación de proyectos; él puede dar información como: contraseñas, proveedor de servicio, aplicaciones, etc. Todo elemento incautado, debe ser fotografiado durante el proceso, así como verificar el nivel de batería y ser registrado todo. Finalmente, al no ser un delito penal ya que en esos casos criminales es necesario obtener huellas digitales no es necesario manipular los elementos con guantes de látex.

Los dispositivos incautados fueron: teléfono celular marca Samsung Galaxy J1 Ace, batería, memoria externa SD, cable USB y cargador como se observa en las Figuras 6.4, 6.2, 6.3. El nivel de batería es superior al 50 % por lo que no es necesario apagar el dispositivo. No se realizan fotografías de la memoria externa SD y la SIM, debido a que se debe desconectar la batería y esto causaría que se pierda información de la memoria RAM.

(a) Cara frontal. (b) Cara posterior.

Figura 6.2: Dispositivo móvil marca Samsung.

(a) Cable USB marca Samsung.

(b) Cargador marca Samsung.

Figura 6.3: Cable USB y cargador del teléfono celular.

Figura 6.4: Accesorio (estuche).

Existen casos donde por falla de dispositivo móvil o algún agente externo la batería no tiene una larga duración. En estos casos es necesario que el dispositivo sea transferido al laboratorio de manera inmediata y no perder datos alojada en la memoria RAM. La información en cuanto a batería se puede conseguir en la entrevista con el propietario del móvil.

6.3.3. Seguridad y traslado

De la misma forma de la sub-sección anterior se da seguimiento a las tareas, en la Figura 6.5 se encierra en el cuadro rojo y azul las tareas de medidas de seguridad y transporte de evidencia respectivamente.

Medidas de seguridad

Es necesario documentar todas las actividades que se van a realizar mediante un registro donde se apunta el lugar, la hora de la actividad y el personal responsable. Cada uno de los elementos incautados deben ser empaquetados, transportados y almacenados, así como asegurarlos. Por otra parte, también deben tener una adecuada identificación y etiquetado. Para todos estos

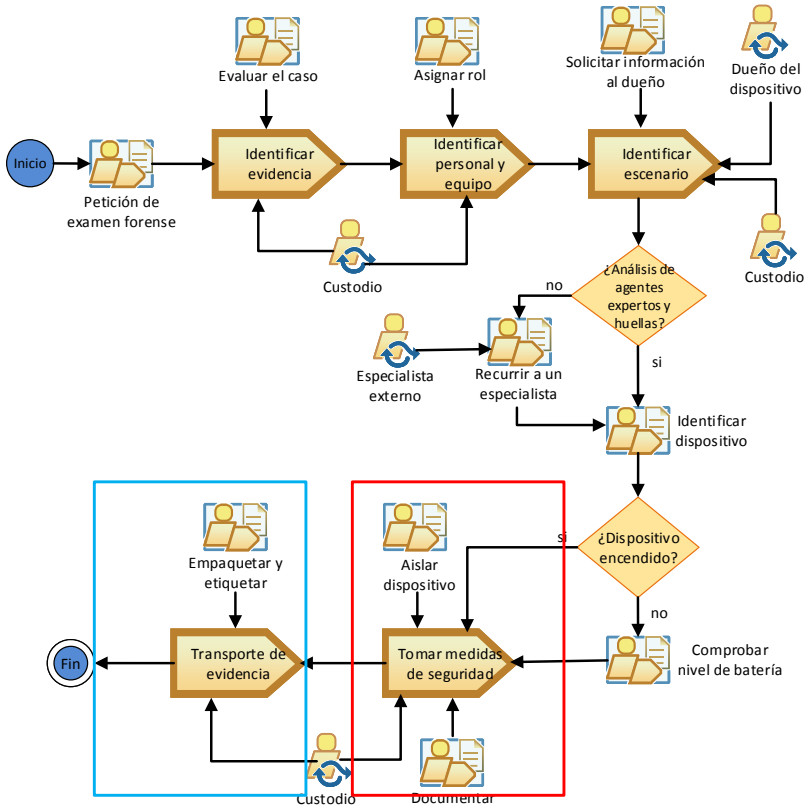


Figura 6.5: Medidas de seguridad y transporte de la evidencia.

puntos se deben considerar mecanismos de empaquetado anti-estático y hermético. El dispositivo, cable, cargador y accesorios se colocarán en bolsas separadas, luego deben ser empaquetados y sellados en una bolsa hermética, ésta debe ser guardada en un contenedor llamado jaula de Faraday el cual aísla las radiofrecuencias y evitar comunicaciones con algún dispositivo. Se observa en la Figura 6.6 un ejemplo de esta jaula o se puede aislar el dispositivo con papel aluminio si no se consigue este tipo de elementos. Finalmente, se debe etiquetar correctamente y documentar.

Figura 6.6: Jaula de Faraday. Fuente [6].

Transporte de evidencia

Luego el empaqueta dela evidencia se traslada al laboratorio o un lugar seguro donde se pueda proseguir con la cadena de custodia. Se deben tomar en cuenta algunos factores a evitar para el transporte de la evidencia como: golpes, presión excesiva, temperatura muy alta o baja y exceso de humedad. La evidencia se debe almacenar en un espacio seguro y adecuado con todos los equipos y herramientas que se van a utilizar; este perímetro debe estar restringido.

6.4. Adquisición

La segunda fase del poseso se muestra en la Figura 6.7 y se da seguimiento de las tareas que se van desarrollando, en el cuadro azul se encierra la recepción del paquete que contiene la evidencia que se explica en la sub-sección 6.4.1; mientras que, el cuadro rojo muestra la identificación de la evidencia que se detalla en la sub-sección 6.4.2.

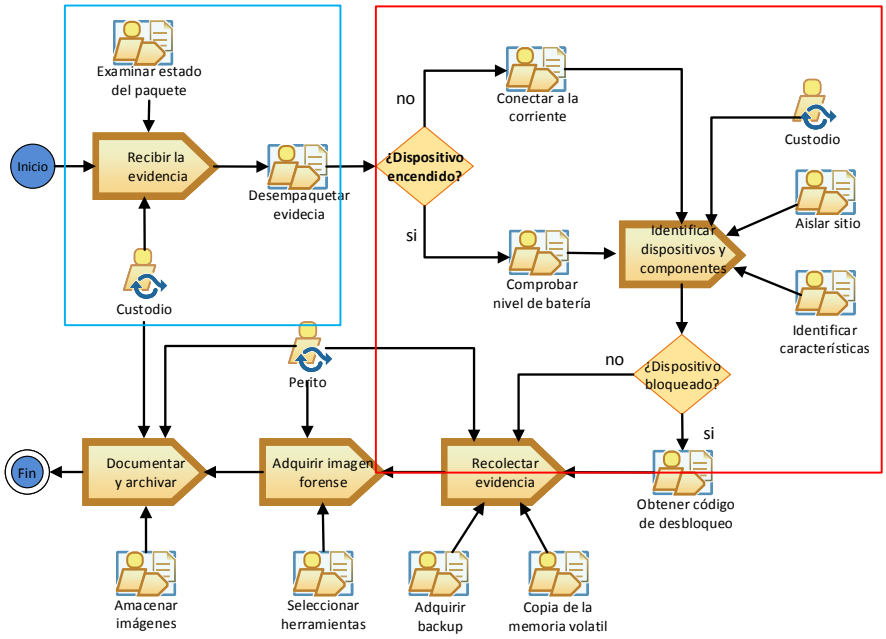


Figura 6.7: Recepción e identificación de la evidencia.

En la adquisición o recolección de la evidencia electrónica, el perito encargado debe contar con las herramientas especializadas y un lugar de trabajo que cumpla con las normas necesarias. Durante la investigación, el perito se puede encontrar con varios obstáculos que deben ser

solucionados siguiendo un proceso y tomando en cuenta las buenas prácticas propuestas por los estándares, normas y leyes. Al adquirir la información digital el perito debe cumplir con: principio de imparcialidad y no alterar la o las pruebas obtenidas.

6.4.1. Recepción

El laboratorio en donde se va a extraer la evidencia digital del teléfono incautado debe estar equipado con las herramientas forenses necesarias, estar aislado de señales externas esto se los puede realizar con inhibidores de señal. Cuando el paquete es recibido este deber examinado para confirmar si llegó en buenas condiciones, caso contrario si hubo alguna alteración, pérdida o manipulación de cualquier naturaleza deberá ser documentado. Finalmente, se registra la fecha y hora en que llego, así como los datos del encargado.

6.4.2. Identificación del dispositivo

Cuando el dispositivo y sus componentes se encuentran en el sitio donde van a ser analizados y este cumple con las respectivas seguridades, se procede a desempaquetar teniendo en cuenta que todo debe ser manejado con cautela. Además, se verifica si el nivel de batería es mayor a 50 % caso contrario se deberá conectar a la corriente el dispositivo para que éste no se apague; todos estos pasos deben ser registrados mediante fotografías y estar bien documentados en un registro de actividades.

Para este caso se pide información al estudiante del tipo de dispositivo que posee como: marca, version del dispositivo, si acaso el cable y cargador son originales, estado en que se encuentra, versión de sistema operativo y código de desbloqueo. Con todos esta información se puede obtener la Tabla 6.1 con un resumen de los datos más relevantes para la investigación.

6.4.3. Recolección de evidencia

Una vez identificados todos los elementos que intervendrán en la investigación y al ser una prueba de concepto se obtuvo las contraseñas mediante la entrevista con el usuario del teléfono, debido a que está bloqueado con un código de 4 dígitos (PIN).

Se procede a realizar un *backup* mediante ADB, para poder saber que comando se deben utilizar mediante la consola de comando con digital *adb help* como se ve en la Figura 6.8, de esta forma se tiene el comando y una explicación de su función.

Tabla 6.1: Características básicas de los dispositivos

Dispositivo	Marca	Características
Teléfono	Samsung	Galaxy J1 Ace Pantalla 4.3 pulgadas Procesador Dual Core, 512 RAM Camara Dual de 5MP y 2MP Sistema Operativo V 4.4.4 Operador Movistar Número: 0987935551 Almacenamiento interno 4GB
Batería	Samsung	3.8V -6.84Wh - 2600mAh
Memoria Extraible	Kingston	SD-CO2G
Cable USB	Samsung	Original Color blanco
Cargador	Samsung	Original, buen estado Color blanco
Accesorio	Desconocido	Estuche

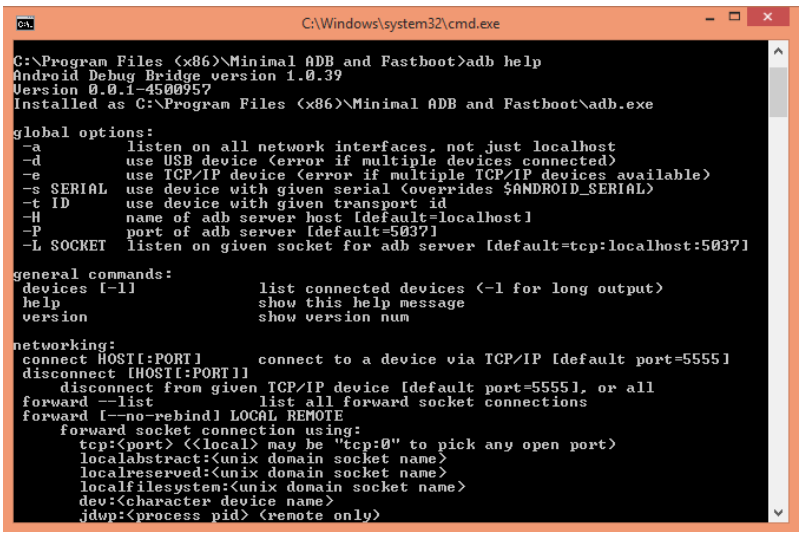


Figura 6.8: Consola para ejecutar ADB

Para realizar el *backup* primero se conecta el dispositivo al equipo (computador) mediante el cable de datos USB, segundo se procede a escribir la siguiente línea de comando.

```
adb backup [-f <file>] [-apk|-noapk] [-shared|-noshared] [-all] [-system|nosystem]
```

La copia se guarda como SM-J110H en un computador al que tendrá acceso solo el perito. De ser necesario el *backup* se realizará ante notario, esto asegurará que no se haya alterado la

evidencia. A continuación se procede a explicar en la Tabla 6.2 cada unos de los comandos que pueden ser utilizados para crear otras copias o guardar información específica.

Tabla 6.2: Descripción de los principales comandos

-f <file>	La dirección donde se almacena la copia de seguridad
-apk|-noapk	Incluir o no configuraciones o apks
-shared|-nochared	La copia del contenido de la targeta SD activar/desactivar
-all	Todas las aplicaciones en el dispositivo instaladas
-system|nosystem	Aplicaciones del sistema del dispositivo
<packages>	Como comando extra este puede especificar donde buscar algun dato específico

Una vez obtenida la copia de seguridad como se observa en la Figura 6.9, se debe asegurar la integridad de ésta. Se busca el *hash1* y *md5* del *backup* mediante la herramienta MD5Summer [30]. En el Apéndice C se detalla la obtención de el HASH.

SHA1: dd7a3ef60bc14487bd88f921d9010d127a100e2bm
MD5: e5fab6a6ad410dbc8c5fe3fd25422031

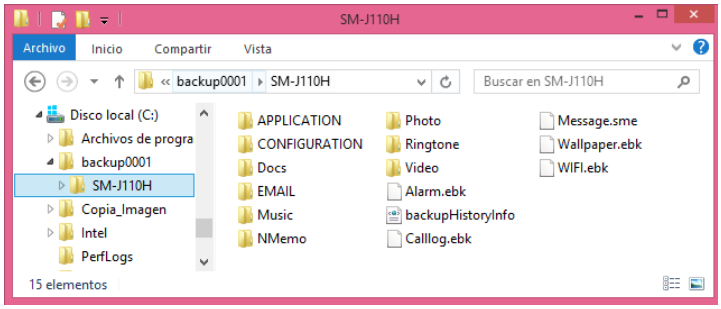


Figura 6.9: Backup del teléfono marca Samsung

Existen otras técnicas para obtener el *backup* como la herramienta oficial de la marca del dispositivo que se va a analizar. Como es en este caso Samsung proporciona en su página Smart Switch [96].

6.4.4. Extracción de imagen forense

De igual manera al paso realizado en el punto anterior, donde se realiza el *backup* del teléfono, se escoge las herramientas que serán de utilidad para realizar este paso. Como se ha comentado anteriormente existe varias herramientas, pero se escoge las más relevantes para la extracción de información del usuario como son: Andriller, [31], Oxigen forensic [29] y MOBILedit [30], esto luego de analizar en cada uno de ellos la información que entrega de los dispositivos móviles (esto puede obtener de las características de cada software). Además, se ha utilizado más de un software debido al aporte de cada uno de ellos en determinados temas, así al extraer información de varios software y correlacionar los eventos, se tiene una evidencia completa.

Cada una de las imágenes forenses extraídas de cada herramienta se guardan en la ruta *-f C:/Copia_imagen/nombreherramienta*. Como una buena práctica de prevención de perdida de información por parte del investigador se debe crear un respaldo de cada imagen. Para obtener más detalles de la forma de adquirir dichas imágenes, todo los pasos están detallados en el Informe Pericial en el Apéndice C.

6.4.5. Documentación y archivo

Se documentan todos los procedimientos para el informe técnico como son: nombre y dirección de la información copiada, herramientas utilizadas, comandos, características del dispositivos y accesorios, captura de pantalla de la información obtenida mediante las herramientas, observaciones, etc. También para este informe es de ayuda gráficos o tablas resumen para analizar la información

6.5. Análisis

En esta fase lo primero que se debe realizar con la evidencia recolectada es crear varias copias o imágenes forenses de respaldo, de esta forma evitar pérdida de información. Ahora, ya con los respaldos, se procede a una revisión técnica mas detallada. Debido a los grandes volúmenes de datos durante la extracción es necesario llevar esto a una forma y tamaño que se pueda manipular, paro esto se efectúa filtrado de información, búsqueda por palabras, validación de datos, fecha, hora. La información eliminada también es de gran importancia aun que esta tarea se puede volver tediosa. Todos los datos recuperados dependerán de la herramienta forense que se utiliza y sus capacidades. Estas tareas antes descrita, se facilitará con la utilización de la herramienta de registro de actividades.

Para seguir el proceso del capítulo 4 en la Figura 6.10 se muestra los pasos a seguir. En el cuadro azul se encierra la tarea de extracción de la sub-sección 6.5.1 y en el cuadro rojo la tarea de análisis de información de la 6.5.2.

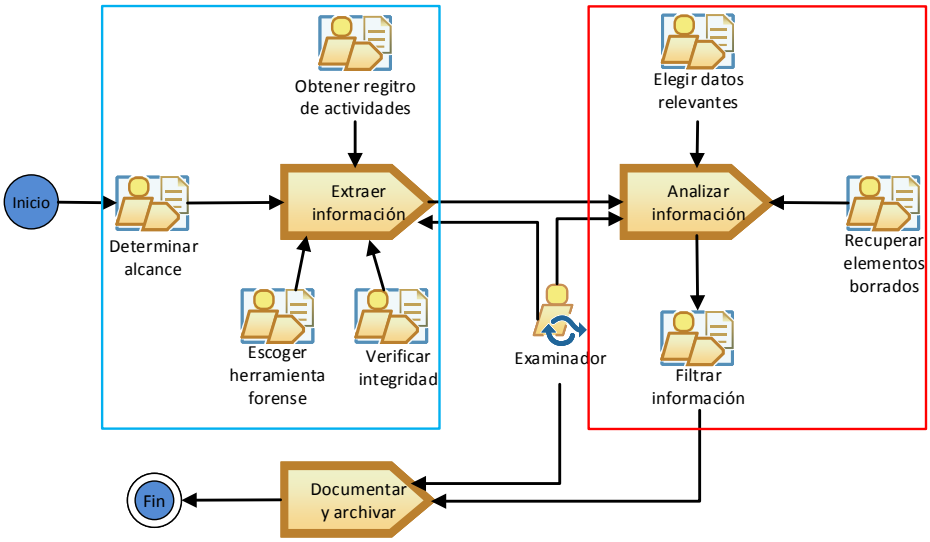


Figura 6.10: Extracción y análisis de información.

6.5.1. Extracción de la información mediante herramientas

Con la imagen obtenida de Andriller, Oxygen Forensic y MOBILedit; se procede a extraer los archivos de interés con ayuda de los reportes que generan los programas como son: Andriller, Oxygen Forensinc, MOBILedit, Autopsy, Bulk extractor y Kali Linux. Para las tres primeras herramientas se debe escoger los reportes excel; mientras que, para el resto de herramientas por defecto los reportes están en archivos texto. El proceso de extracción y obtención de informe de cada herramienta se detalla en el Apéndice C.

Por otra parte, para conocer la composición del sistema de ficheros se ingresa en la consola de ADB *adb shell* como se muestra en la Figura 6.11 y se verifica la ruta de la información que se va analizar como se observa en la misma Figura 6.11. Pero al no contar con acceso *root* debido a que se tendría que apagar el teléfono y perder información alojada en la RAM, se tiene acceso a los archivos descargas, historial, llamadas, mensajes, almacenamiento, etc.

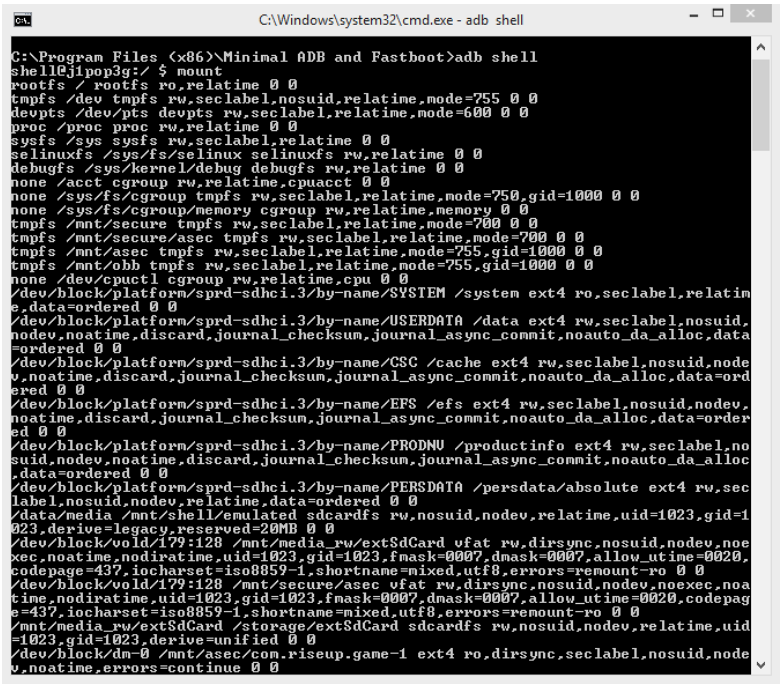


Figura 6.11: Composición de sistema de ficheros.

Una vez obtenidos los reportes se procede a utilizar la herramienta desarrollada en el capítulo 5 RegistroActividades. Los reportes generados en total son 26 y cada uno posee gran cantidad de información. Analizar cada uno de estos reportes es una tarea larga y tediosa ya que se debe buscar una fecha y hora en particular. En este punto RegistroActividades ayuda a reducir el tiempo de la investigación devolviendo solamente las actividades que competen a este caso. El reporte final de la herramienta RegistroActividades se lo puede estudiar con mas detalle en el Apéndice B.

6.5.2. Análisis de las actividades del usuario

El objetivo de este proceso es identificar las características que se relacionan con el caso, identificar los posibles eventos involucrados que perjudicaron al objeto en un tiempo determinado. Con toda la información recolectada mediante los reportes generados por cada software, se procede a unirlos en un solo documento el cual contendrá las actividades que el usuario a realizado en su teléfono como son: llamadas, mensajes, descargas, sitios visitados, aplicaciones utilizadas entre otras actividades.

El reunir los datos en un sólo informe general no solo ayuda al investigador a revisar las

actividades en el dispositivo, sino a simplificar el tiempo así como tener un análisis completo de cada archivo existente en el fichero. Si se desea contar con un análisis mas profundo de un dato en particular encontrado en el informe de actividades, el mismo informe proporciona la dirección donde se encuentra alojada esta información y mediante un herramienta forense se la examinará.

6.5.3. Documentación y archivo

Esta paso se ha separado debido su importancia, se debe realizar durante todo el proceso de análisis de evidencia. Se protege esta evidencia digital mediante la cadena de custodia bien documentada, esto ayuda a que no se generan pruebas que invaliden la evidencia o que ha sido modificada de alguna manera. Se utilizan formularios y registros para identificar las acciones realizadas, el encargado y la hora y fecha en las que se realizan.

6.6. Reporte

Los informes que se realizan en esta fase son trámites que poco tienen que ver con el proceso técnico, sino mas bien un proceso para documentar y organizar la información. Esta última fase es una revisión que proporciona la validación del proceso, identificar pasos que se pueden mejorar, resultados e interpretación de estos. Como se ha mencionando, estos documentos deben ser claros y concisos, teniendo en cuenta que el informe técnico va dirigido hacia departamentos de sistemas, investigadores forenses y personal jurídico.

El Consejo de la Judicatura [94] proporciona un formato de informe pericial el cual servirá de guía para realizar el informe pericial (ver Apéndice C).

6.7. Resultados

En esta sección del capítulo de dan a conocer los resultados más importantes de la prueba de concepto poniendo énfasis en los resultados que arrojó la herramienta RegistroActividades. Además, se analiza las actividades más relevantes del caso para la presentación del informe pericial.

6.7.1. Identificación y preservación de la evidencia

La primera fase del proceso es muy importante debido a que es el punto de partida para la investigación. En está fase se determina la estrategia que se va a seguir durante el caso, así como el personal que va intervenir y el rol que cada uno va a desarrollar. Ésto ayuda a que la investigación sea ordenada y poder actuar ante un contra tiempo de forma eficiente.

Por otra parte, se obtuvo información importante como: los dispositivos que serán analizados, las características de cada uno y los materiales que van a intervenir en la investigación.

6.7.2. Adquisición de la evidencia

En esta fase se obtiene la mayor cantidad de información proveniente del dispositivo móvil de la forma menos invasiva posible. Se emplea herramientas forenses para la extracción tanto en Windows como en Linux, los reportes obtenidos se observan en la Figura 6.12; en total fueron 26 archivos adquiridos.

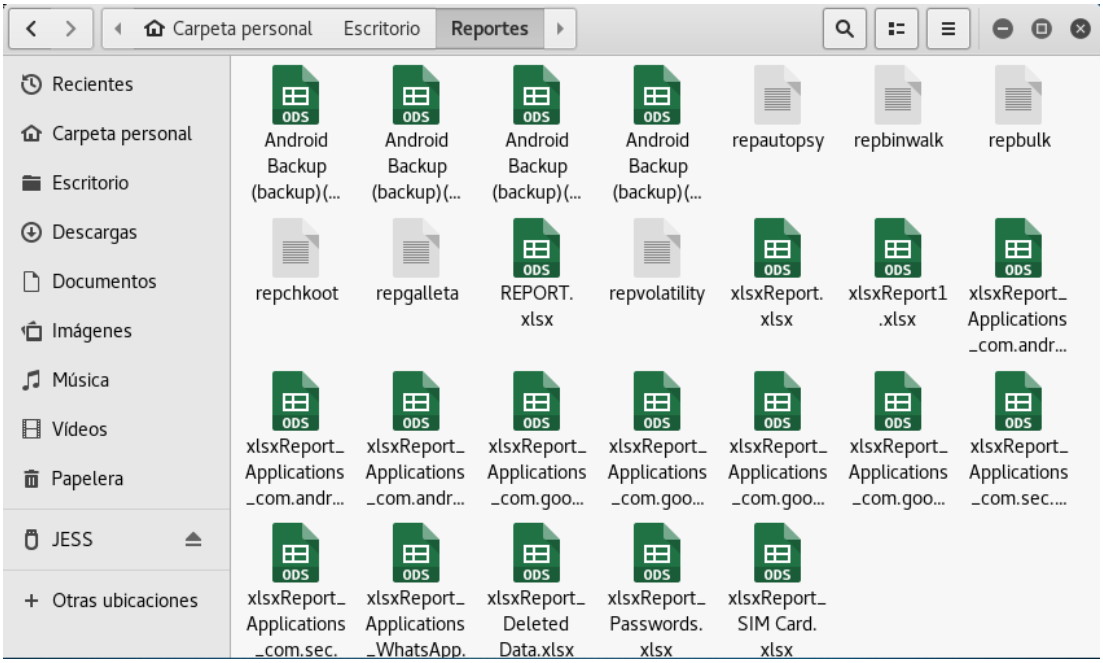


Figura 6.12: Reportes obtenidos mediante herramientas forenses.

La herramienta desarrollada permite al investigador recolectar la información de cada reporte obtenido ingresando la fecha del día 9 de julio de 2018 entre las 11h00 a 13h00, en la Figura 6.13

se observa que se obtuvo 283 actividades. El reporte completo de lo puede ver en el Apéndice B.

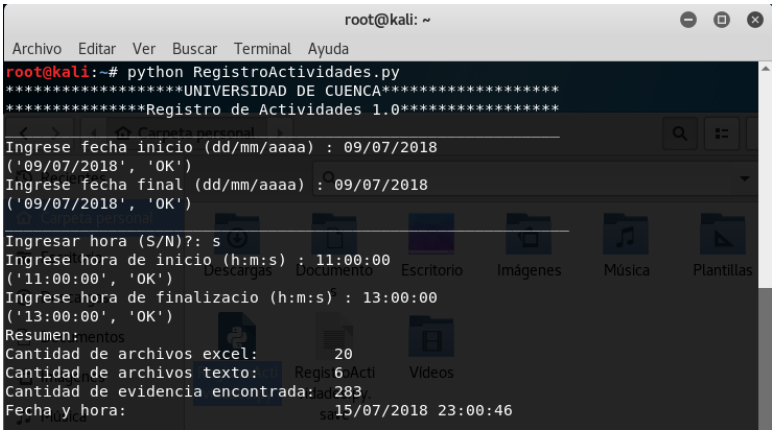


Figura 6.13: Resultados obtenidos de RegistroActividades.

Con este reporte, el siguiente paso en obtener las actividades más relevantes. Para ésto se estudia el documento y se obtienen los datos que estén relacionados con el tema del examen que el docente preparó. En la Figura 6.14 se ingresan los códigos de las actividades referente al caso planteado.

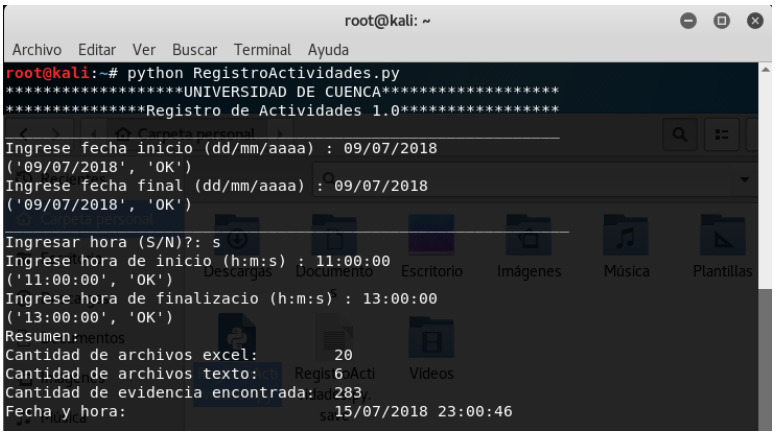


Figura 6.14: Resultados filtrados obtenidos de RegistroActividades.

6.7.3. Análisis de la evidencia

En esta sección se presenta lo más relevante para el caso planteado en un principio; es decir, las actividades que el dueño del dispositivo realizó durante el periodo que duró el examen.

Se ha dividido en cinco diferentes tipos de evidencia que son: historial de navegación web, cookies, imágenes, descargas y aplicaciones de mensajería instantánea. Finalmente, los procesos del sistema también son descritos, pero con el fin de establecer que hubo actividad del teléfono.

En cuanto a el historial de navegación, se encontraron 11 páginas web las cuales por su etiqueta (título de la página web) se relacionan con el tema de la asignatura. En cuanto a las cookies existen 8 actividades que dejaron rastro sobre las páginas que el usuario deseaba acceder. Por otra parte, las 4 imágenes que se lograron recuperar gracias a la dirección que el registro provee también arrojan información pertinente al caso. Finalmente, se obtuvo un intento de descarga de un archivo PDF y se envió un audio mediante la aplicación de mensajería WhatsApp.

En total fueron 25 actividades que el investigador determinó que son de importancia y que argumentan que el estudiante cometió copia durante el examen. Para ver con más detalle todos estas pruebas ver Apéndice C, donde se encuentra el informe pericial detallando cada una de las tareas desarrolladas a lo largo del capítulo.

Capítulo 7

Conclusiones y Recomendaciones

En este capítulo se presentan las conclusiones finales del trabajo realizado así como la interpretación de los resultados obtenidos a lo largo del trabajo, las limitaciones que se encontraron en el proceso, y finalmente, se proponen maneras de ampliar la investigación a futuro.

7.1. Conclusiones

La informática forense orientada al análisis de dispositivos móviles es uno de los campos que requiere mayor investigación debido a que éstos dispositivos han tenido gran acogida en el mundo, provocando así que cualquier persona disponga de uno o más dispositivos móviles. Uno de los aspectos de mayor importancia y una de las bases de la misma, es la recolección de datos en un dispositivo inteligente ya que contienen gran información de las actividades que realiza el usuario, lo que les convierten a estos dispositivos en una fuente de evidencia digital. Finalmente, la informática forense hace que esta información cobre valor legal y pueda ser relevante ante un proceso jurídico.

De manera que, el objeto de estudio de este trabajo de titulación, es el desarrollo de una herramienta y un proceso de cómo debe llevar a cabo una investigación forense digital en dispositivos móviles orientando la investigación a dispositivos Android, ya que, hasta el momento no existe una herramienta forense que recolecte toda la evidencia digital en un solo reporte final el cual se presenta como un registro de actividades.

Teniendo esto en consideración, se procede a analizar y determinar el correcto proceso forense que permita al investigador identificar las tareas a seguir, desde el momento en el que se incauta un dispositivo celular inteligente con sistema operativo Android para su respectiva investigación hasta la elaboración del informe pericial. Este proceso permite identificar, preservar, recolectar y analizar adecuadamente la evidencia digital.

Según los objetivos propuestos en el primer capítulo se concluye:

- Con respecto al objetivo 1, se realizó un mapeo sistemático de la literatura de cómo se está llevando los procesos de una investigación forense proveniente de dispositivos móviles, esta investigación arrojó resultados como: dónde está la evidencia digital, tipo de evidencia, la manera de cómo tratarla, herramientas para la extracción, todos estos resultados han sido la base para el trabajo de titulación.
- Con respecto al objetivo 2, en el capítulo 4 se desarrolló un proceso que permitió adquirir, manejar y analizar información digital almacenada en el dispositivo celular móvil, de ésta manera garantizar la investigación. Este proceso se llevó a cabo identificando los principales estándares tanto nacionales como internacionales y varias herramientas forenses.
- Con respecto al objetivo 3, para el desarrollo del proceso se tuvo que analizar y repasar las normas y estándares tanto nacionales como internacionales, para que sirvan de base al momento de efectuar el proceso adecuado para el manejo de evidencia digital acorde a las normas y leyes estatales
- El objetivo 4, fue conseguido al crear satisfactoriamente una propuesta de herramienta “ RegistroActividades”, la cual contribuye a automatizar y reducir tiempo de análisis de la

evidencia. El seleccionar las herramientas adecuadas para la adquisición de evidencia que sirve como entrada para la aplicación, representa una pieza crucial de la investigación, sin embargo, ninguna de ellas posee la capacidad de adquirir toda la información del dispositivo; por tanto, es necesario utilizar varias de ellas para mejorar el resultado, así como en el análisis. Finalmente, la ventaja de utilizar el lenguaje de programación Python que es de código abierto para el desarrollo de la herramienta, es verificar el código fuente y así validar que éste no altere la evidencia digital.

- El objetivo 5, fue conseguido realizando una prueba de conceptos basada en el escenario propuesto y presentando los resultados más relevantes en un apartado. Esta prueba permite evaluar la usabilidad de la herramienta RegistroActividades y por consecuencia brindar recomendaciones y mejorar dicha herramienta.

Como se puede observar los objetivos de la tesina fueron abarcados en su totalidad y vale la pena destacar que a nivel académico se ha logrado un claro entendimiento del tema. También gracias al desarrollo del trabajo se llegó a las siguientes conclusiones:

Una de las dificultad que se encontró durante la ejecución del presente trabajo, ha sido el hecho de conseguir acceso al terminal móvil sin conocer las contraseñas de desbloqueo. Puede parecer una simpleza, sin embargo, se han dedicado varias horas de búsqueda y prueba de diversos métodos, que en principio permitían realizar un desbloqueo de la pantalla del dispositivo sin que este deba ser apagado. Finalmente, se llegó a la conclusión que con versiones superiores de Android 5.0 no existe una forma sencilla, o al menos gratuita de conseguirlo. La solución a este problema, es conseguir dichos códigos mediante la entrevista con el dueño del dispositivo o en otro caso realizar un estudio más profundo sobre este tema.

Por otra parte, con las herramientas *software* que se escogieron se puede llevar a cabo una gran cantidad de actividades relacionadas con la extracción de evidencia digital. Además, este tipo de herramientas son fáciles de utilizar ya que son intuitivas y no suelen requerir conocimientos extensos por parte del perito. Luego de realizar un análisis bibliográfico, y un análisis de los aspectos técnicos que varios *software* ofrecen, se determinó que para este trabajo se utilicen *software* de tipo comerciales y de licencia libre. Las herramientas comerciales fueron obtenidas mediante licencias *trial*; es decir, la empresa que maneja estos *software* otorgó una licencia por un lapso no mayor a 20 días dependiendo de la herramienta. Se debe considerar que fue un corto tiempo para las pruebas con dichas herramientas.

Las *software* forenses instalados en Windows poseen una interfaz amigable para el usuario, mientras que, los instalados en Linux se ejecutan por medio comando en la terminal. Sin embargo, en términos de procesamiento y obtención de resultados no hay diferencia más que la amigabilidad de la herramienta.

Según la cantidad de información que el usuario tenga almacenado un su móvil, el tiempo de extracción del *backup* y la imagen forense del dispositivo podría tomar de algunos minutos a varias horas. Por otro lado, el tiempo de procesamiento de la herramienta RegistroActividades no supera los 20 minutos, comparado al tiempo que un investigador le toma realizar un análisis forense para encontrar evidencia.

Otro aspecto a tener en consideración con respecto a la herramienta desarrollada en el capítulo 5, fue la dificultad de trabajar con dos tipos de archivos debido a su diferente composición a la hora de presentar los resultados. El reporte que arroja la herramienta puede ser mejorado en su presentación, para que no solo el investigador pueda entenderlo sino para personal jurídico.

Se ha tenido en cuenta que el proceso y herramienta en conjunto se pueden evaluar no solo con una prueba de concepto, sino ponerlos en práctica en un caso de estudio que demuestre que los pasos a seguir definidos en el proceso permitan evaluar la usabilidad tanto del proceso como de la herramienta.

Luego también se ha tenido en cuenta el producto final, el cual va dirigido a investigadores que tengan que analizar grandes volúmenes de datos en casos donde se deba realizar un análisis de las actividades que un usuario desarrolla en un dispositivo.

Además, se ha estudiado en qué consisten las soluciones de seguridad propietarias como Samsung KNOX y qué niveles de seguridad ofrecen. Tanto las medidas de seguridad propias de Android como las propietarias de los diferentes fabricantes de teléfonos móviles, son de gran ayuda para proporcionar un nivel de seguridad mucho mayor al usuario. Sin embargo, añaden nuevas dificultades a la investigación digital forense que debemos afrontar y para las que debemos buscar soluciones con urgencia.

Como se puede observar los objetivos del trabajo de titulación fueron abarcados en su totalidad y cabe destacar que a nivel académico se ha logrado un claro entendimiento del tema.

7.2. Recomendaciones

Existen diferentes variables que pueden ser mejoradas en estudios posteriores y que no fueron tomadas en cuenta en el presente trabajo por ser un primer estudio para el análisis en dispositivos móviles. A continuación, se presentan las principales:

- Se sugiere ampliar el trabajo orientado al análisis forense y seguridad informática, de esta manera reforzar nuevos campos de investigación.
- En el paso de incautación del dispositivo, se debe solicitar al dueño del dispositivo mó-

vil más información de este. Se puede realizar entrevistas para conseguir el número de teléfono, claves de desbloqueo y así agilizar la investigación.

- En el desarrollo del programa se debe tener conocimiento en programación y un buen manejo de la sintaxis de lenguaje.

7.3. Trabajos Futuros

En esta sección, se explica cómo se podrían aplicar los resultados obtenidos y cómo estos pueden ser mejorados o ampliados con futuras investigaciones.

- El trabajo presentado, da un primer enfoque sobre el manejo de evidencia digital en dispositivos móviles con SO Android, éste posteriormente puede ser desarrollado para otros sistemas operativos como iOS y Windows Phone, dado que estos SO también tienen una gran acogida de acuerdo a la investigación realizada.
- Se ve también necesario para futuros trabajos mejorar la herramienta desarrollada, ésto se lograría no sólo utilizando seis tipos de *software* para la extracción de evidencia, si no ampliar el número de este modo tener un registro de actividades amplio y más detallado.
- Otro aspecto necesario para realizarlo en un futuro es el refinamiento del proceso de investigación forense en dispositivos móviles mediante la evaluación de un mayor número de normas y estándares.
- Se espera también realizar en un futuro más de una prueba de concepto o en el mejor de los escenarios un caso de estudio enfocado a la obtención de actividades.

Bibliografía

[1] R. Hernández Sampieri, C. Fernández Collado, y P. Baptista Lucio, "Metodología de la investigación," 2010.

[2] M. Song, W. Xiong, y X. Fu, "Research on architecture of multimedia and its design based on android," in *Internet Technology and Applications, 2010 International Conference on.* IEEE, 2010, pp. 1–4.

[3] T.-M. Gronli, J. Hansen, G. Ghinea, y M. Younas, "Mobile application platform heterogeneity: Android vs windows phone vs ios vs firefox os," in *Advanced Information Networking and Applications (AINA), 2014 IEEE 28th International Conference on.* IEEE, 2014, pp. 635–641.

[4] I. N. d. E. y. Censos. Tecnologías de la información y comunicación (TIC) – 2014. [En línea]. Disponible: http://www.ecuadorencifras.gob.ec/tecnologias-de-la-informacion-y-comunicacion-tic-2014/

[5] 2017: A year of mixed results in the latin american smartphone market. [En línea]. Disponible: https://www.counterpointresearch.com/2017-year-mixed-results-latin-american-smartphone-market/

[6] StrongHold faraday. [En línea]. Disponible: https://www.paraben.com/product-categories/stronghold-faraday

[7] K. Hayson, K.-P. Chow, y M. Y. Kwan, "The next generation for the forensic extraction of electronic evidence from mobile telephones," in *Systematic Approaches to Digital Forensic Engineering (SADFE), 2013 Eighth International Workshop on.* IEEE, 2013, pp. 1–7.

[8] M. Chernyshev, S. Zeadally, Z. Baig, y A. Woodward, "Mobile forensics: Advances, challenges, and research opportunities," *IEEE Security & Privacy*, vol. 15, num. 6, pp. 42–51, 2017.

[9] K. Barmpatsalou, D. Damopoulos, G. Kambourakis, y V. Katos, "A critical review of 7 years of mobile device forensics," *Digital Investigation*, vol. 10, num. 4, pp. 323–349, 2013.

[10] Y.-C. Tso, S.-J. Wang, C.-T. Huang, y W.-J. Wang, "iphone social networking for evidence investigations using itunes forensics," in *Proceedings of the 6th International Conference on Ubiquitous Information Management and Communication*. ACM, 2012, p. 62.

[11] F. J. De León Huerta, "Estudios de metodologías de análisis forense digital," 2009.

[12] M. Taylor, G. Hughes, J. Haggerty, D. Gresty, y P. Almond, "Digital evidence from mobile telephone applications," *Computer Law & Security Review*, vol. 28, num. 3, pp. 335–339, 2012.

[13] ISO/IEC 27037:2012 - information technology – security techniques – guidelines for identification, collection, acquisition and preservation of digital evidence. [En línea]. Disponible: https://www.iso.org/standard/44381.html

[14] T. Killalea y D. Brezinski. Guidelines for evidence collection and archiving. [En línea]. Disponible: https://tools.ietf.org/html/rfc3227

[15] AENOR. AENOR: Norma UNE 71505-1:2013. [En línea]. Disponible: http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0051411

[16] Ecuador. Leyes y Reglamentos, *Código orgánico integral penal*. Ministerio de Justicia, Derechos Humanos y Cultos, OCLC: 946324729.

[17] d. C. E. Ley, "Ley de comercio electrónico, firmas electrónicas y mensajes de datos," *C. NACIONAL, Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos*, p. 21, 2002.

[18] C. Gervilla Rivas, "Metodología para un análisis forense," 2014.

[19] M. López Delgado, "Análisis forense digital," *España: Red Iris*, 2007.

[20] J. Garrido, "Análisis forense digital en entornos windows," 2014.

[21] J. Cano y J. Jeimy, "Computación forense descubriendo los rastros informáticos," *Computación forense descubriendo los rastros informáticos. Editorial: AlfaOmega, México*, pp. 1–7, 2009.

[22] M. Gorricho Moreno y J. L. Gorricho Moreno, *Comunicaciones móviles*. Edicions UPC, 2002.

[23] M. R. Bhalla y A. V. Bhalla, "Generations of mobile wireless technology: A survey," *International Journal of Computer Applications*, vol. 5, num. 4, 2010.

[24] O. Okediran, O. Arulogun, R. Ganiyu, y C. Oyeleye, "Mobile operating systems and application development platforms: A survey," *International Journal of Advanced Networking and Applications*, vol. 6, num. 1, p. 2195, 2014.

[25] M. G. Temperini, "Delitos informáticos en latinoamérica: un estudio de derecho comparado," in *XLIII Jornadas Argentinas de Informática e Investigación Operativa (43JAIIO)-XIV Simposio Argentino de Informática y Derecho (SID)(Buenos Aires, 2014)*, 2014.

[26] E. Observatorio. Delitos informáticos y comercio electrónico en ecuador. [En línea]. Disponible: http://oiprodat.com/2013/03/06/delitos-informaticos-y-comercio-electronico-ecuador/

[27] P. N. d. Ecuador. Delitos informáticos o ciberdelitos. [En línea]. Disponible: http://www.policiaecuador.gob.ec/delitos-informaticos-o-ciberdelitos/

[28] G. F. Limodio, D. A. Herrera, N. G. A. Cossari, y M. J. A. Miño, "El uso de software abierto para el análisis de la evidencia digital," p. 8.

[29] Oxygen forensics - mobile forensics solutions: software and hardware. [En línea]. Disponible: https://www.oxygen-forensic.com/es/

[30] Home of the MD5summer. [En línea]. Disponible: http://www.md5summer.org/

[31] Andriller | android forensic tools. [En línea]. Disponible: https://www.andriller.com/

[32] Autopsy – download | autopsy. [En línea]. Disponible: https://www.autopsy.com/download/

[33] Index of /downloads/bulk_extractor. [En línea]. Disponible: http://downloads.digitalcorpora.org/downloads/bulk_extractor/

[34] Our most advanced penetration testing distribution, ever. [En línea]. Disponible: https://www.kali.org/

[35] OWASP. [En línea]. Disponible: https://www.owasp.org/index.php/Main_Page

[36] md5deep and hashdeep. [En línea]. Disponible: http://md5deep.sourceforge.net/

[37] Download android studio and SDK tools. [En línea]. Disponible: https://developer.android.com/studio/

[38] N. Scrivens y X. Lin, "Android digital forensics: data, extraction and analysis," in *Proceedings of the ACM Turing 50th Celebration Conference-China*. ACM, 2017, p. 26.

[39] R. Al Mushcab y P. Gladyshev, "Forensic analysis of instagram and path on an iphone 5s mobile device," in *Computers and Communication (ISCC), 2015 IEEE Symposium on*. IEEE, 2015, pp. 146–151.

[40] T. B. Tajuddin y A. A. Manaf, "Forensic investigation and analysis on digital evidence discovery through physical acquisition on smartphone," in *Internet Security (WorldCIS), 2015 World Congress on*. IEEE, 2015, pp. 132–138.

[41] B. Kitchenham, "Procedures for performing systematic reviews," *Keele, UK, Keele University*, vol. 33, num. 2004, pp. 1–26, 2004.

[42] B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey, y S. Linkman, "Systematic literature reviews in software engineering–a systematic literature review," *Information and software technology*, vol. 51, num. 1, pp. 7–15, 2009.

[43] C. Sanchez, P. Cedillo, y A. Bermeo, "A systematic mapping study for intelligent user interfaces-iui," in *Information Systems and Computer Science (INCISCOS), 2017 International Conference on*. IEEE, 2017, pp. 361–368.

[44] P. Cedillo, A. Fernandez, E. Insfran, y S. Abrahão, "Quality of web mashups: a systematic mapping study," in *International Conference on Web Engineering*. Springer, 2013, pp. 66–78.

[45] M. Szvetits y U. Zdun, "Systematic literature review of the objectives, techniques, kinds, and architectures of models at runtime," *Software & Systems Modeling*, vol. 15, num. 1, pp. 31–69, 2016.

[46] K. Petersen, R. Feldt, S. Mujtaba, y M. Mattsson, "Systematic mapping studies in software engineering." in *EASE*, vol. 8, 2008, pp. 68–77.

[47] K. Petersen, S. Vakkalanka, y L. Kuzniarz, "Guidelines for conducting systematic mapping studies in software engineering: An update," *Information and Software Technology*, vol. 64, pp. 1–18, 2015.

[48] N. Alherbawi, Z. Shukur, y R. Sulaiman, "Systematic literature review on data carving in digital forensic," *Procedia Technology*, vol. 11, pp. 86–92, 2013.

[49] S. Alharbi, J. Weber-Jahnke, y I. Traore, "The proactive and reactive digital forensics investigation process: A systematic literature review," in *International Conference on Information Security and Assurance*. Springer, 2011, pp. 87–100.

[50] T. M. Robinson y C. Clemens, "Service-learning and forensics: A systematic literature review," *The Forensic of Pi Kappa Delta*, vol. 99, pp. 35–49, 2014.

[51] D. Walnycky, I. Baggili, A. Marrington, J. Moore, y F. Breitinger, "Network and device forensic analysis of android social-messaging applications," *Digital Investigation*, vol. 14, pp. S77–S84, 2015.

[52] K. Zatyko y J. Bay, "The digital forensics cyber exchange principle," *Forensic Magazine*, pp. 13–5, 2011.

[53] T. Alyahya y F. Kausar, "Snapchat analysis to discover digital forensic artifacts on android smartphone," *Procedia Computer Science*, vol. 109, pp. 1035–1040, 2017.

[54] C. Anglano, "Forensic analysis of whatsapp messenger on android smartphones," *Digital Investigation*, vol. 11, num. 3, pp. 201–213, 2014.

[55] C. Anglano, M. Canonico, y M. Guazzone, "Forensic analysis of telegram messenger on android smartphones," *Digital Investigation*, vol. 23, pp. 31–49, 2017.

[56] H.-C. Chu, C.-H. Lo, y H.-C. Chao, "The disclosure of an android smartphone's digital footprint respecting the instant messaging utilizing skype and msn," *Electronic Commerce Research*, vol. 13, num. 3, pp. 399–410, 2013.

[57] M. I. Husain y R. Sridhar, "iforensics: forensic analysis of instant messaging on smart phones," in *International Conference on Digital Forensics and Cyber Crime*. Springer, 2009, pp. 9–18.

[58] L. Chen y Y. Mao, "Forensic analysis of email on android volatile memory," in *Trustcom/-BigDataSE/I SPA, 2016 IEEE*. IEEE, 2016, pp. 945–951.

[59] G. B. Satrya, P. T. Daely, y M. A. Nugroho, "Digital forensic analysis of telegram messenger on android devices," in *Information & Communication Technology and Systems (ICTS), 2016 International Conference on*. IEEE, 2016, pp. 1–7.

[60] A. Shortall y M. H. B. Azhar, "Forensic acquisitions of whatsapp data on popular mobile platforms," in *Emerging Security Technologies (EST), 2015 Sixth International Conference on*. IEEE, 2015, pp. 13–17.

[61] S. Varma, R. J. Walls, B. Lynn, y B. N. Levine, "Efficient smart phone forensics based on relevance feedback," in *Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices*. ACM, 2014, pp. 81–91.

[62] S. Omeleze y H. S. Venter, "Testing the harmonised digital forensic investigation process model-using an android mobile phone," in *Information Security for South Africa, 2013*. IEEE, 2013, pp. 1–8.

[63] M. Yates y H. Chi, "A framework for designing benchmarks of investigating digital forensics tools for mobile devices," in *Proceedings of the 49th Annual Southeast Regional Conference*. ACM, 2011, pp. 179–184.

[64] A. Mylonas, V. Meletiadis, B. Tsoumas, L. Mitrou, y D. Gritzalis, "Smartphone forensics: A proactive investigation scheme for evidence acquisition," in *IFIP International Information Security Conference*. Springer, 2012, pp. 249–260.

[65] A. Mylonas, V. Meletiadis, L. Mitrou, y D. Gritzalis, "Smartphone sensor data as digital evidence," *Computers & Security*, vol. 38, pp. 51–75, 2013.

[66] N. Al Mutawa, I. Baggili, y A. Marrington, "Forensic analysis of social networking applications on mobile devices," *Digital Investigation*, vol. 9, pp. S24–S33, 2012.

[67] C. Ntantogian, D. Apostolopoulos, G. Marinakis, y C. Xenakis, "Evaluating the privacy of android mobile applications under forensic analysis," *Computers & Security*, vol. 42, pp. 66–76, 2014.

[68] S. Yadav, K. Ahmad, y J. Shekhar, "Analysis of digital forensic tools and investigation process," in *High Performance Architecture and Grid Computing*. Springer, 2011, pp. 435–441.

[69] A. K. Kubi, S. Saleem, y O. Popov, "Evaluation of some tools for extracting e-evidence from mobile devices," in *Application of Information and Communication Technologies (AICT), 2011 5th International Conference on*. IEEE, 2011, pp. 1–6.

[70] R. J. S. Rueda y B. D. W. Rico, "Defining of a practical model for digital forensic analysis on android device using a methodology post-mortem," in *Telematics and Information Systems (EATIS), 2016 8th Euro American Conference on*. IEEE, 2016, pp. 1–5.

[71] F. Amato, G. Cozzolino, A. Mazzeo, y N. Mazzocca, "Correlation of digital evidences in forensic investigation through semantic technologies," in *Advanced Information Networking and Applications Workshops (WAINA), 2017 31st International Conference on*. IEEE, 2017, pp. 668–673.

[72] F. Cohen, "Two models of digital forensic examination," in *Systematic Approaches to Digital Forensic Engineering, 2009. SADFE'09. Fourth International IEEE Workshop on*. IEEE, 2009, pp. 42–53.

[73] J. Rahaditya, A. Gde, A. Sasmita, G. Made, E. Pratama, y I. P. Agus, "Prototyping sms forensic tool application based on digital forensic research workshop 2001 (dfrws) investigation model: Case study: Sms togel in indonesia," in *Information Technology Systems and Innovation (ICITSI), 2016 International Conference on*. IEEE, 2016, pp. 1–6.

[74] K. M. Ovens y G. Morison, "Identification and analysis of email and contacts artefacts on ios and os x," in *Availability, Reliability and Security (ARES), 2016 11th International Conference on*. IEEE, 2016, pp. 321–327.

[75] S. O'shaughnessy y A. Keane, "Impact of cloud computing on digital forensic investigations," in *IFIP International Conference on Digital Forensics*. Springer, 2013, pp. 291–303.

[76] P. Sharma, D. Arora, y T. Sakthivel, "Mobile cloud forensic: Legal implications and counter measures," in *International Conference on Information and Communication Technology for Intelligent Systems*. Springer, 2017, pp. 531–542.

[77] Forensic toolkit. [En línea]. Disponible: https://accessdata.com/product-download/mobile-phone-examiner-plus-mpe-5.5.4

[78] Forensic toolkit. [En línea]. Disponible: https://accessdata.com/products-services/forensic-toolkit-ftk

[79] UFED.com. [En línea]. Disponible: http://ufed.com/

[80] H. Jahankhani y A. Azam, "Review of forensic tools for smartphones," in *EC2ND 2006*. Springer, 2007, pp. 69–84.

[81] Welcome to magnet forensics. [En línea]. Disponible: https://www.magnetforensics.com/

[82] Digital forensics training | incident response training | SANS. [En línea]. Disponible: https://digital-forensics.sans.org/

[83] The sleuth kit (TSK) & autopsy: Open source digital forensics tools. [En línea]. Disponible: https://www.sleuthkit.org/

[84] e-fense :: Cyber security & computer forensics software. [En línea]. Disponible: http://www.e-fense.com/helix3pro.php

[85] Live view. [En línea]. Disponible: http://liveview.sourceforge.net/

[86] Katana forensics - mobile forensics software and services. [En línea]. Disponible: https://katanaforensics.com/

[87] Programas de ElcomSoft para recuperar contraseñas, forenses, programas de seguridad de sistemas: recuperar o reajustar la contraseña perdida u olvidada, quitar protección, desbloquear el sistema. [En línea]. Disponible: https://www.elcomsoft.es/

[88] G. Grispos, W. B. Glisson, y T. Storer, "Using smartphones as a proxy for forensic evidence contained in cloud storage services," in *System Sciences (HICSS), 2013 46th Hawaii International Conference on*. IEEE, 2013, pp. 4910–4919.

[89] K. Hajdarevic y V. Dzaltur, "An approach to digital evidence collection for successful forensic application: An investigation of blackmail case," in *Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2015 38th International Convention on*. IEEE, 2015, pp. 1387–1392.

[90] M. Harbawi y A. Varol, "An improved digital evidence acquisition model for the internet of things forensic i: A theoretical framework," in *Digital Forensic and Security (ISDFS), 2017 5th International Symposium on*. IEEE, 2017, pp. 1–6.

[91] NIST | national institute of standards and technology. [En línea]. Disponible: https://www.nist.gov/national-institute-standards-and-technology

[92] SWGDE. [En línea]. Disponible: https://www.swgde.org/

[93] About the software & systems process engineering metamodel specification version 2.0. [En línea]. Disponible: https://www.omg.org/spec/SPEM

[94] Consejo de la judicatura | consejo de la judicatura. [En línea]. Disponible: http://funcionjudicial.gob.ec/

[95] A. Marzal y I. G. Luengo, *Introducción a la Programación con Python y C.* Publicacions de la Universitat Jaume I, 2002.

[96] Smart switch | samsung soporte españa. [En línea]. Disponible: //www.samsung.com/es/support/smart-switch/

Anexos

Apéndice A

Solicitud de examen forense

SOLICITUD DE EXAMEN FORENSE

Fecha de solicitud: 09/07/2018

Jessica Camacho

Se solicita la realización del examen forense digital, al dispositivo celular móvil en posesión de Juan Perez, marca Samsung, modelo J1 Ace 4GB (SM-J110H/DS), FCC ID: A3LSMJ110H, color blanco.

1. **Antecedentes:**
   El examen realizado a los estudiantes de octavo nivel de la asignatura de Organización y Evaluación de Proyectos de la facultad de Ingeniería de la Universidad XYZ, en el horario de 11h00 a 13h00 el 9 de julio de 2018.

   Antes de iniciar el examen el profesor encargado expuso que, no está permitido el usos de ningún tipo de ayuda ya sea apuntes, libros, calculadora, computador y/o celular; de ser el caso se retirará el examen y se procede a suspensión en dicha materia. Durante el transcurso del examen el docente notó que un estudiante realizó un movimiento sospechoso, al ver esto el docente se acercó al estudiante y verificó que poseía un dispositivo móvil escondido, por lo que se le pidió al estudiante entregar el examen y retirarse.

   Ante este contratiempo el estudiante afirma que no realizó ningún intento de copia, si no que solamente saco su teléfono para ver la hora y verificar el tiempo que le quedaba hasta la finalización del examen.

   El docente solicita incautar el dispositivo para determinar las actividades que realizó durante el examen, de este modo verificar si están relacionadas con el tema de la asignatura. Para dicho fin se solicita desarrollar un análisis forense al dispositivo móvil del estudiante.

2. **Elementos a determinar:**
   Actividades que se desarrollan en el dispositivo el día 9 de julio de 2018 en horario de clases.
3. **Autorizaciones:**
   Otorgar acceso root al dispositivo SI ( ) NO (x)

   Extracción de información SI (x) NO ( )

Se ha informado sobre el procedimiento y su importancia para la investigación y se otorga de manera libre el consentimiento y autorización legar. Se hace constar que el documento ha sido leído y consecuentemente entendido por mí en su total integridad.

Autoriza

Firma: Juan Perez

Nombres y Apellidos: Juan Pedro Perez López

CI: 0102587889

Se compromete a cumplir la persona o institución auditora con los artículos, de acuerdo al marco legal del país.

Apéndice B

Reporte final: actividades de un usuario

Este apéndice se encuentra el reporte completo obtenido de la herramienta RegistroActividades.py.

ra101 Fecha: 2018-07-09 11:26:44 Etiqueta: /Stored Audio Detalles: /Stored Audio/AUD-20180709-WA0000.opus AUD-20180709-WA0000.opus image phone/applications0/com.whatsapp/live_specific/Media/WhatsApp Audio/AUD-20180709-WA0000.opus 124103

ra102 Fecha: 2018-07-09 11:39:38 Etiqueta: osp.db Detalles: filesystem phone/applications0/com.osp.app.signin/backup/db/osp.db 28672

ra103 Fecha: 2018-07-09 11:39:39 Etiqueta: alarm.db Detalles: filesystem phone/applications0/com.sec.android.app.clockpackage/backup/db/alarm.db 20480

ra104 Fecha: 2018-07-09 11:39:52 Etiqueta: LOG Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/File System/Origins/LOG 304

ra105 Fecha: 2018-07-09 11:40:34 Etiqueta: que es pim - Buscar con Google Detalles: false https://www.google.com.ec/search?q=que+es+pim&oq=que+es+pim&aqs=chrome..69i57.5378j0j4&client=ms-android-samsung&sourceid=chrome-mobile&ie=UTF-8 1 com.android.chrome

ra106 Fecha: 2018-07-09 11:40:35 Etiqueta: cfd27fb28d0a9fac_0 Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/GPUCache/cfd27fb28d0a9fac_0 1575

ra107 Fecha: 2018-07-09 11:40:48 Etiqueta: 9ff50baef471748b_0 Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Service Worker/ScriptCache/9ff50baef471748b_0 25058

ra108 Fecha: 2018-07-09 11:40:48 Etiqueta: 9ff50baef471748b_1 Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Service Worker/ScriptCache/9ff50baef471748b_1 36571

ra109 Fecha: 2018-07-09 11:40:48 Etiqueta: LOG.old Detalles: filesystem phone/applications0/com.android.chrome/backup/rapp_chrome/Default/IndexedDB/https_dentially.info_0.indexeddb.leveldb/LOG.old 366

ra110 Fecha: 2018-07-09 11:41:18 Etiqueta: 29abb1c1d5088b28_0 Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/GPUCache/29abb1c1d5088b28_0 2150

ra111 Fecha: 2018-07-09 11:42:02 Etiqueta: content_store.db Detalles: filesystem phone/applications0/com.google.android.googlequicksearchbox/backup/r/app_si/now_content_store/content_store.db 57344

ra112 Fecha: 2018-07-09 11:42:02 Etiqueta: content_store.db-shm Detalles: filesystem phone/applications0/com.google.android.googlequicksearchbox/backup/r/app_si/now_content_store/content_store.db-shm 32768

ra113 Fecha: 2018-07-09 11:42:02 Etiqueta: content_store.db-wal Detalles: filesystem phone/applications0/com.google.android.googlequicksearchbox/backup/r/app_si/now_content_store/content_store.db-wal 0

ra114 Fecha: 2018-07-09 11:42:09 Etiqueta: LOG Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/IndexedDB/https_dentially.info_0.indexeddb.leveldb/LOG 366

ra115 Fecha: 2018-07-09 11:42:09 Etiqueta: 4e4357bbba41752a_0 Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Service Worker/ScriptCache/4e4357bbba41752a_0 25058

ra116 Fecha: 2018-07-09 11:42:09 Etiqueta: 4e4357bbba41752a_1 Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Service Worker/ScriptCache/4e4357bbba41752a_1 36571

ra117 Fecha: 2018-07-09 11:42:20 Etiqueta: 000003.log Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Service Worker/Database/000003.log 45593

ra118 Fecha: 2018-07-09 11:42:56 Etiqueta: 933904bac1dbffa6_0 Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/GPUCache/933904bac1dbffa6_0 2235

ra119 Fecha: 2018-07-09 11:42:56 Etiqueta: 9368c4ec6b3167ef_0 Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/GPUCache/9368c4ec6b3167ef_0 1833

ra120 Fecha: 2018-07-09 11:43:19 Etiqueta: Detalles: false https://www.google.com.ec/amp/s/www.gladysgbegnedji.com/planificar-la-respuesta-a-los-riesgos-2/amp/ 1 com.android.chrome

ra121 Fecha: 2018-07-09 11:43:30 Etiqueta: QuotaManager Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/QuotaManager 57344

ra122 Fecha: 2018-07-09 11:43:30 Etiqueta: QuotaManager-journal Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/QuotaManager-journal 0

ra123 Fecha: 2018-07-09 11:43:39 Etiqueta: a8a2b8006f2f7766_0 Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/GPUCache/a8a2b8006f2f7766_0 1629

ra124 Fecha: 2018-07-09 11:43:40 Etiqueta: 4506735a10a1a8d9_0 Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/GPUCache/4506735a10a1a8d9_0 1776

ra125 Fecha: 2018-07-09 11:43:43 Etiqueta: 7a71e93f5ebe3fed_0 Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/GPUCache/7a71e93f5ebe3fed_0 1187

ra126 Fecha: 2018-07-09 11:43:52 Etiqueta: planificar las resouestas a.los riesgos - Buscar con Google Detalles: false https://www.google.com.ec/search?q=planificar+las+resouestas+a.los+riesgos&oq=planificar+las+resouestas+a.los+riesgos&aqs=chrome..69i57j0l3.23500j0j9&client=ms-android-samsung&sourceid=chrome-mobile&ie=UTF-8 2 com.android.chrome

ra127 Fecha: 2018-07-09 11:46:32 Etiqueta: 642f367f1cf70515_0 Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/GPUCache/642f367f1cf70515_0 2181

ra128 Fecha: 2018-07-09 11:47:49 Etiqueta: 3.- La interacción entre los procesos de la Dirección de Proyectos según La guía del PMBOK® 26-03-2012 – 1ra Parte / La Guía del PMBOK® / Capitulo 3 | formulaproyectosurbanospmipe Detalles: false https://formulaproyectosurbanospmipe.wordpress.com/2012/04/25/3-la-interaccion-entre-los-procesos-de-la-direccion-de-proyectos-segun-la-guia-del-pmbok-26-03-2012-1ra-parte-la-guia-del-pmbok-capitulo-3/ 1 com.android.chrome

ra129 Fecha: 2018-07-09 11:48:35 Etiqueta: event_generator.xml Detalles: filesystem phone/applications0/com.android.vending/backup/sp/event_generator.xml 122

ra130 Fecha: 2018-07-09 11:48:36 Etiqueta: scheduler Detalles: filesystem phone/applications0/com.android.vending/backup/db/scheduler20480

ra131 Fecha: 2018-07-09 11:48:36 Etiqueta: finsky.xml Detalles: filesystem phone/applications0/com.android.vending/backup/sp/finsky.xml31712

ra132 Fecha: 2018-07-09 11:48:37 Etiqueta: localappstate.db Detalles: filesystem phone/applications0/com.android.vending/backup/db/localappstate.db 1470464

ra133 Fecha: 2018-07-09 11:48:37 Etiqueta: localappstate.db-journal Detalles: filesystem phone/applications0/com.android.vending/backup/db/localappstate.db-journal 119528

ra134 Fecha: 2018-07-09 11:48:45 Etiqueta: phenotype.db Detalles: filesystem phone/applications0/com.android.vending/backup/db/phenotype.db 245760

ra135 Fecha: 2018-07-09 11:48:45 Etiqueta: phenotype.db-shm Detalles: filesystem phone/applications0/com.android.vending/backup/db/phenotype.db-shm 32768

ra136 Fecha: 2018-07-09 11:48:45 Etiqueta: phenotype.db-wal Detalles: filesystem phone/applications0/com.android.vending/backup/db/phenotype.db-wal 0

ra137 Fecha: 2018-07-09 11:49:33 Etiqueta: 192b63747196de2e_0 Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/GPUCache/192b63747196de2e_0 1838

ra138 Fecha: 2018-07-09 11:49:33 Etiqueta: e49bfecd850bbcd0_0 Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/GPUCache/e49bfecd850bbcd0_0 1712

ra139 Fecha: 2018-07-09 11:49:42 Etiqueta: f1a5d9ca190117b9_0 Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/GPUCache/f1a5d9ca190117b9_0 1871

ra140 Fecha: 2018-07-09 11:49:43 Etiqueta: 2042621ecce1d831_0 Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/GPUCache/2042621ecce1d831_02230

ra141 Fecha: 2018-07-09 11:49:43 Etiqueta: 354dc64e7e1dbc96_0 Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/GPUCache/354dc64e7e1dbc96_0 2161

ra142 Fecha: 2018-07-09 11:49:45 Etiqueta: 06f6435a243693a0_0 Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/GPUCache/06f6435a243693a0_0 1541

ra143 Fecha: 2018-07-09 11:51:18 Etiqueta: internal.db-shm Detalles: filesystem phone/applications0/com.android.providers.media/backup/db/internal.db-shm 32768

ra144 Fecha: 2018-07-09 11:51:29 Etiqueta: Detalles: false https://formulaproyectosurbanospmipe.files.wordpress.com/2012/04/b3.jpg 1 com.android.chrome

ra145 Fecha: 2018-07-09 11:51:32 Etiqueta: eucookielaw Detalles: false formulaproyectosurbanospmipe.wordpress.com / 1546706985699 com.android.chrome

ra146 Fecha: 2018-07-09 11:51:32 Etiqueta: personalized-ads-consent Detalles: false formulaproyectosurbanospmipe.wordpress.com / 1546706985699 com.android.chrome

ra147 Fecha: 2018-07-09 11:51:32 Etiqueta: eucookielaw Detalles: false formulaproyectosurbanospmipe.wordpress.com / 1546706985699 com.android.chrome

ra148 Fecha: 2018-07-09 11:51:32 Etiqueta: personalized-ads-consent Detalles: false formulaproyectosurbanospmipe.wordpress.com / 1546706985699 com.android.chrome

ra149 Fecha: 2018-07-09 11:51:34 Etiqueta: Detalles: false https://www.google.com.ec/search?q=interaccion+entre+los+grupos+de+procesos+en+un+proyecto&client=ms-android-samsung&source=lnms&tbm=isch&sa=X&ved=0ahUKEwi-3rWJx6HcAhWBrFkKHZ4SBZwQ_AUICCgB&biw=320&bih=452#imgrc=sUZ-4sxtkAKSyM%3A 2 com.android.chrome

ra150 Fecha: 2018-07-09 11:51:37 Etiqueta: interaccion entre los grupos de procesos en un proyecto - Buscar con Google Detalles: false https://www.google.com.ec/search?q=interaccion+entre+los+grupos+de+procesos+en+un+proyecto&client=ms-android-samsung&source=lnms&tbm=isch&sa=X&ved=0ahUKEwi-3rWJx6HcAhWBrFkKHZ4SBZwQ_AUICCgB&biw=320&bih=452 2 com.android.chrome

ra151 Fecha: 2018-07-09 11:51:42 Etiqueta: interaccion entre los grupos de procesos en un proyecto - Buscar con Google Detalles: false https://www.google.com.ec/search?client=ms-android-samsung&q=interaccion+entre+los+grupos+de+procesos+en+un+proyecto&oq=interaccion+entre+los+grupos+de+procesos+en+un+proyecto&aqs=mobile-gws-lite.....3 2 com.android.chrome

ra152 Fecha: 2018-07-09 11:52:40 Etiqueta: 3fc64126717849b5_0 Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/GPUCache/3fc64126717849b5_0 2183

ra153 Fecha: 2018-07-09 11:52:40 Etiqueta: 64912e18c1ab1bb8_0 Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/GPUCache/64912e18c1ab1bb8_0 2180

ra154 Fecha: 2018-07-09 11:52:40 Etiqueta: 7ab5aafa2925813c_0 Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/GPUCache/7ab5aafa2925813c_0 2157

ra155 Fecha: 2018-07-09 11:52:40 Etiqueta: db907e85d9e0f02c_0 Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/GPUCache/db907e85d9e0f02c_0 2217

ra156 Fecha: 2018-07-09 11:52:40 Etiqueta: f7e9341235221bfe_0 Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/GPUCache/f7e9341235221bfe_0 2108

ra157 Fecha: 2018-07-09 11:55:44 Etiqueta: 20180709_115544.jpg Detalles: filesystem phone/applications0/1/backup/DCIM/Camera/20180709_115544.jpg 2791430

ra158 Fecha: 2018-07-09 11:55:44 Etiqueta: 20180709_115544.jpg Detalles: false filesystem phone/applications0/1/backup/DCIM/Camera/20180709_115544.jpg 2791430 2560 pixel 1536 pixel SAMSUNG SM-J110H

ra159 Fecha: 2018-07-09 11:55:59 Etiqueta: 20180709_115559.jpg Detalles: filesystem phone/applications0/1/backup/DCIM/Camera/20180709_115559.jpg 2557267

ra160 Fecha: 2018-07-09 11:55:59 Etiqueta: 20180709_115559.jpg Detalles: false filesystem phone/applications0/1/backup/DCIM/Camera/20180709_115559.jpg 2557267 2560 pixel 1536 pixel 270° SAMSUNG SM-J110H

ra161 Fecha: 2018-07-09 11:56:23 Etiqueta: 20180709_115623.jpg Detalles: filesystem phone/applications0/1/backup/DCIM/Camera/20180709_115623.jpg 2926813

ra162 Fecha: 2018-07-09 11:56:23 Etiqueta: 20180709_115623.jpg Detalles: false filesystem phone/applications0/1/backup/DCIM/Camera/20180709_115623.jpg 2926813 2560 pixel 1536 pixel SAMSUNG SM-J110H

ra163 Fecha: 2018-07-09 11:56:36 Etiqueta: CURRENT Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Session Storage/CURRENT 16

ra164 Fecha: 2018-07-09 11:56:36 Etiqueta: LOCK Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Session Storage/LOCK 0

ra165 Fecha: 2018-07-09 11:56:36 Etiqueta: LOG Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Session Storage/LOG 128

ra166 Fecha: 2018-07-09 11:56:36 Etiqueta: MANIFEST-000001 Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Session Storage/MANIFEST-000001 41

ra167 Fecha: 2018-07-09 11:57:12 Etiqueta: Identificación de riesgos en proyectos. Qué es y técnicas para hacerla. Detalles: false https://www.recursosenprojectmanagement.com/identificacion-de-riesgos/ 1 com.android.chrome

ra168 Fecha: 2018-07-09 11:57:36 Etiqueta: 002465.log Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Local Storage/leveldb/002465.log 35646

ra169 Fecha: 2018-07-09 11:57:36 Etiqueta: 000003.log Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Session Storage/000003.log 255

ra170 Fecha: 2018-07-09 11:58:44 Etiqueta: the-real-index Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Service Worker/ScriptCache/index-dir/the-real-index 576

ra171 Fecha: 2018-07-09 11:59:10 Etiqueta: __cfduid Detalles: false .creativecommons.org / d1225021b94048bf3010cff5c96d41bb71517931134 com.android.chrome

ra172 Fecha: 2018-07-09 11:59:10 Etiqueta: __cfduid Detalles: false .creativecommons.org / d1225021b94048bf3010cff5c96d41bb71517931134 com.android.chrome

ra173 Fecha: 2018-07-09 12:00:20 Etiqueta: 20180709_120020.jpg Detalles: filesystem phone/applications0/1/backup/DCIM/Camera/20180709_120020.jpg 2294454

ra174 Fecha: 2018-07-09 12:00:20 Etiqueta: 20180709_120020.jpg Detalles: false filesystem phone/applications0/1/backup/DCIM/Camera/20180709_120020.jpg 2294454 2560 pixel 1536 pixel SAMSUNG SM-J110H

ra175 Fecha: 2018-07-09 12:00:53 Etiqueta: LOG.old Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Download Service/EntryDB/LOG.old 148

ra176 Fecha: 2018-07-09 12:00:53 Etiqueta: LOG.old Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/NTPSnippets/images/LOG.old 148

ra177 Fecha: 2018-07-09 12:00:53 Etiqueta: LOG.old Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/NTPSnippets/snippets/LOG.old 148

ra178 Fecha: 2018-07-09 12:00:53 Etiqueta: LOG.old Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Sync Data/LevelDB/LOG.old 303

ra179 Fecha: 2018-07-09 12:00:53 Etiqueta: 000025.ldb Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/data_reduction_proxy_leveldb/000025.ldb 220

ra180 Fecha: 2018-07-09 12:00:53 Etiqueta: LOG.old Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/data_reduction_proxy_leveldb/LOG.old 264

ra181 Fecha: 2018-07-09 12:00:54 Etiqueta: LOG.old Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Feature Engagement Tracker/AvailabilityDB/LOG.old 351

ra182 Fecha: 2018-07-09 12:00:54 Etiqueta: LOG.old Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Feature Engagement Tracker/EventDB/LOG.old 337

ra183 Fecha: 2018-07-09 12:00:54 Etiqueta: LOG.old Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Service Worker/Database/LOG.old 315

ra184 Fecha: 2018-07-09 12:00:54 Etiqueta: _ga Detalles: false .www.recursosenprojectmanagement.com / GA1.3.10170594.1531155399 com.android.chrome
ra185 Fecha: 2018-07-09 12:00:54 Etiqueta: _gid Detalles: false .www.recursosenprojectmanagement.com / GA1.3.810849174.1531155399 com.android.chrome
ra186 Fecha: 2018-07-09 12:00:54 Etiqueta: _ga Detalles: false .www.recursosenprojectmanagement.com / GA1.3.10170594.1531155399 com.android.chrome
ra187 Fecha: 2018-07-09 12:00:54 Etiqueta: _gid Detalles: false .www.recursosenprojectmanagement.com / GA1.3.810849174.1531155399 com.android.chrome
ra188 Fecha: 2018-07-09 12:01:05 Etiqueta: 96fb4b58a3d7f518_0 Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/GPUCache/96fb4b58a3d7f518_0 2249

ra189 Fecha: 2018-07-09 12:02:02 Etiqueta: Detalles: false https://www.google.com.ec/search?q=identificacion+de+riesgos&oq=identificacion+de+riesgos&aqs=chrome..69i57j0l3.9070j0j9&client=ms-android-samsung&sourceid=chrome-mobile&ie=UTF-8#imgrc=9-SwZ7VVUuKhNM%3A 1 com.android.chrome
ra190 Fecha: 2018-07-09 12:02:13 Etiqueta: 4d787e89df07e032_0 Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/GPUCache/4d787e89df07e032_02438

ra191 Fecha: 2018-07-09 12:03:19 Etiqueta: Detalles: false https://www.google.com.ec/search?q=identificacion+de+riesgos&client=ms-android-samsung&source=lnms&tbm=isch&sa=X&ved=0ahUKEwis-cLxyKHcAhXRjVkKHXwzDWUQ_AUICCgB&biw=320&bih=452#imgrc=9-SwZ7VVUuKhNM%3A1 com.android.chrome
ra192 Fecha: 2018-07-09 12:03:47 Etiqueta: identificacion de riesgos - Buscar con Google Detalles: false https://www.google.com.ec/search?q=identificacion+de+riesgos&client=ms-android-samsung&source=lnms&tbm=isch&sa=X&ved=0ahUKEwis-cLxyKHcAhXRjVkKHXwzDWUQ_AUICCgB&biw=320&bih=452 2 com.android.chrome
ra193 Fecha: 2018-07-09 12:03:53 Etiqueta: identificacion de riesgos - Buscar con Google Detalles: false https://www.google.com.ec/search?q=identificacion+de+riesgos&oq=identificacion+de+riesgos&aqs=chrome..69i57j0l3.9070j0j9&client=ms-android-samsung&sourceid=chrome-mobile&ie=UTF-8 1 com.android.chrome

ra194 Fecha: 2018-07-09 12:04:20 Etiqueta: 3IdentificacíondelosRiesgos_es.pdf Detalles: filesystem phone/applications0/0/backup/Download/3IdentificacíondelosRiesgos_es.pdf 92659

ra195 Fecha: 2018-07-09 12:04:20 Etiqueta: 000003.log Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Feature Engagement Tracker/EventDB/000003.log 467316
ra196 Fecha: 2018-07-09 12:04:20 Etiqueta: download_id_mappings.xml Detalles: filesystem phone/applications0/com.android.chrome/backup/sp/download_id_mappings.xml 279

ra197 Fecha: 2018-07-09 12:04:20 Etiqueta: downloads.db-journal Detalles: filesystem phone/applications0/com.android.providers.downloads/backup/db/downloads.db-journal 0

ra198 Fecha: 2018-07-09 12:04:20 Etiqueta: 3IdentificacíondelosRiesgos_es.pdf Detalles: false application/pdf non-dwnldmngr-download-dont-retry2download 3IdentificacíondelosRiesgos_es.pdf
ra199 Fecha: 2018-07-09 12:04:22 Etiqueta: DocList.db Detalles: filesystem phone/applications0/com.google.android.apps.docs/backup/db/DocList.db 655360

ra200 Fecha: 2018-07-09 12:04:22 Etiqueta: DocList.db-shm Detalles: filesystem phone/applications0/com.google.android.apps.docs/backup/db/DocList.db-shm 32768

ra201 Fecha: 2018-07-09 12:04:22 Etiqueta: DocList.db-wal Detalles: filesystem phone/applications0/com.google.android.apps.docs/backup/db/DocList.db-wal 0

ra202 Fecha: 2018-07-09 12:04:23 Etiqueta: com.google.android.apps.docs_preferences.xml Detalles: filesystem phone/applications0/com.google.android.apps.docs/backup/sp/com.google.android.apps.docs_preferences.xml 1713
ra203 Fecha: 2018-07-09 12:04:23 Etiqueta: com.google.android.gms.analytics.prefs.xml Detalles: filesystem phone/applications0/com.google.android.apps.docs/backup/sp/com.google.android.gms.analytics.prefs.xml 181
ra204 Fecha: 2018-07-09 12:04:24 Etiqueta: phenotype_com.google.apps.drive.android.xml Detalles: filesystem phone/applications0/com.google.android.apps.docs/backup/sp/phenotype_com.google.apps.drive.android.xml 2097

ra205 Fecha: 2018-07-09 12:04:26 Etiqueta: LOG.old Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Local Storage/leveldb/LOG.old 188

ra206 Fecha: 2018-07-09 12:08:07 Etiqueta: in_progress_download_metadata_store Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/in_progress_download_metadata_store 0

ra207 Fecha: 2018-07-09 12:08:22 Etiqueta: google_analytics_v4.db Detalles: filesystem phone/applications0/com.google.android.apps.docs/backup/db/google_analytics_v4.db 28672

ra208 Fecha: 2018-07-09 12:08:22 Etiqueta: google_analytics_v4.db-journal Detalles: filesystem phone/applications0/com.google.android.apps.docs/backup/db/google_analytics_v4.db-journal 12824

ra209 Fecha: 2018-07-09 12:08:23 Etiqueta: 2e11213a2fcadbeb_0 Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/GPUCache/2e11213a2fcadbeb_0 2246

ra210 Fecha: 2018-07-09 12:08:24 Etiqueta: LOG Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Thumbnails/LOG 289

ra211 Fecha: 2018-07-09 12:08:54 Etiqueta: zzzKeyboard_070a_000A_480x296.xml Detalles: filesystem phone/applications0/0/backup/data/zzzKeyboard_070a_000A_480x296.xml 8188

ra212 Fecha: 2018-07-09 12:08:54 Etiqueta: zzzKeyboard_070a_010A_480x296.xml Detalles: filesystem phone/applications0/0/backup/data/zzzKeyboard_070a_010A_480x296.xml 8188

ra213 Fecha: 2018-07-09 12:11:21 Etiqueta: StartupSettings.bin Detalles: filesystem phone/applications0/com.google.android.googlequicksearchbox/backup/r/app_shared_prefs/StartupSettings.bin 54345

ra214 Fecha: 2018-07-09 12:11:31 Etiqueta: phenotype_sharedprefs.xml Detalles: filesystem phone/applications0/com.google.android.play.games/backup/sp/phenotype_sharedprefs.xml 2986

ra215 Fecha: 2018-07-09 12:11:36 Etiqueta: Cookies Detalles: filesystem phone/applications0/com.google.android.googlequicksearchbox/backup/r/app_webview/Cookies 10240

ra216 Fecha: 2018-07-09 12:11:36 Etiqueta: Cookies-journal Detalles: filesystem phone/applications0/com.google.android.googlequicksearchbox/backup/r/app_webview/Cookies-journal 9800

ra217 Fecha: 2018-07-09 12:11:36 Etiqueta: GAPS Detalles: false accounts.google.com / 1:IZkEG9TmaRh4twzYpBfUKbv9OJEC3_6mnEB3t-W-vdBYRV8JKRrcRrWi6dDzS3OMNsyjsfZltKkRi17xbdQ4tcD-JDe9Ag:xcFAQbMW-OHzYLDQ com.google.android.googlequicksearchbox

ra218 Fecha: 2018-07-09 12:11:36 Etiqueta: GAPS Detalles: false accounts.google.com / 1:IZkEG9TmaRh4twzYpBfUKbv9OJEC3_6mnEB3t-W-vdBYRV8JKRrcRrWi6dDzS3OMNsyjsfZltKkRi17xbdQ4tcD-JDe9Ag:xcFAQbMW-OHzYLDQ com.google.android.googlequicksearchbox

ra219 Fecha: 2018-07-09 12:11:53 Etiqueta: content_store.db Detalles: filesystem phone/applications0/com.google.android.googlequicksearchbox/backup/rapp_si/state_dump_event_content_store/content_store.db 77824

ra220 Fecha: 2018-07-09 12:11:53 Etiqueta: content_store.db-shm Detalles: filesystem phone/applications0/com.google.android.googlequicksearchbox/backup/rapp_si/state_dump_event_content_store/content_store.db-shm 32768

ra221 Fecha: 2018-07-09 12:11:53 Etiqueta: content_store.db-wal Detalles: filesystem phone/applications0/com.google.android.googlequicksearchbox/backup/rapp_si/state_dump_event_content_store/content_store.db-wal 41232

ra222 Fecha: 2018-07-09 12:12:01 Etiqueta: Login Data Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Login Data 20480

ra223 Fecha: 2018-07-09 12:12:01 Etiqueta: Login Data-journal Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Login Data-journal 0

ra224 Fecha: 2018-07-09 12:12:01 Etiqueta: 000226.log Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Download Service/EntryDB/000226.log 0

ra225 Fecha: 2018-07-09 12:12:01 Etiqueta: CURRENT Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Download Service/EntryDB/CURRENT 16

ra226 Fecha: 2018-07-09 12:12:01 Etiqueta: LOG Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Download Service/EntryDB/LOG 148

ra227 Fecha: 2018-07-09 12:12:01 Etiqueta: MANIFEST-000225 Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Download Service/EntryDB/MANIFEST-000225 100

ra228 Fecha: 2018-07-09 12:12:01 Etiqueta: 000232.log Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/NTPSnippets/images/000232.log 0

ra229 Fecha: 2018-07-09 12:12:01 Etiqueta: CURRENT Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/NTPSnippets/images/CURRENT 16

ra230 Fecha: 2018-07-09 12:12:01 Etiqueta: LOG Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/NTPSnippets/images/LOG 148

ra231 Fecha: 2018-07-09 12:12:01 Etiqueta: MANIFEST-000231 Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/NTPSnippets/images/MANIFEST-000231 323

ra232 Fecha: 2018-07-09 12:12:01 Etiqueta: 000236.log Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/NTPSnippets/snippets/000236.log 0

ra233 Fecha: 2018-07-09 12:12:01 Etiqueta: CURRENT Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/NTPSnippets/snippets/CURRENT 16

ra234 Fecha: 2018-07-09 12:12:01 Etiqueta: LOG Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/NTPSnippets/snippets/LOG 148

ra235 Fecha: 2018-07-09 12:12:01 Etiqueta: MANIFEST-000235 Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/NTPSnippets/snippets/MANIFEST-000235 202

ra236 Fecha: 2018-07-09 12:12:01 Etiqueta: LOG Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Service Worker/Database/LOG 315

ra237 Fecha: 2018-07-09 12:12:01 Etiqueta: LOG Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Sync Data/LevelDB/LOG 303

ra238 Fecha: 2018-07-09 12:12:01 Etiqueta: 000028.log Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/data_reduction_proxy_leveldb/000028.log 0

ra239 Fecha: 2018-07-09 12:12:01 Etiqueta: CURRENT Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/data_reduction_proxy_leveldb/CURRENT 16

ra240 Fecha: 2018-07-09 12:12:01 Etiqueta: LOG Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/data_reduction_proxy_leveldb/LOG 145

ra241 Fecha: 2018-07-09 12:12:01 Etiqueta: MANIFEST-000027 Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/data_reduction_proxy_leveldb/MANIFEST-000027 241

ra242 Fecha: 2018-07-09 12:12:02 Etiqueta: LOG Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Feature Engagement Tracker/AvailabilityDB/LOG 351

ra243 Fecha: 2018-07-09 12:12:02 Etiqueta: LOG Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Feature Engagement Tracker/EventDB/LOG 337

ra244 Fecha: 2018-07-09 12:12:02 Etiqueta: NID Detalles: false .google.com.ec / 134=d-anHgGSiMd_LT8WjzWqYnI0AYOX401JBbKbE4Hsq-bFVi7WrMezipiXt_rE8EdcAC-JW7e7iLYa4UQ12dwq4pansT5lAaJCMBtEY0TL0Ax6OEb2QpF1f05fJdgJJD3r0-zAzDiUtpnP1ToTWaVAVYFYdnGwFjZ3TnTaKCgjhSwTMnj99slUi4wXHTt_BwSRDTbumrqqtNcPWqrcoNDFgIrLshV6ziYnbfEeeRagkzVGlwYO2zFs_9dk com.android.chrome

ra245 Fecha: 2018-07-09 12:12:02 Etiqueta: NID Detalles: false .google.com.ec / 134=d-anHgGSiMd_LT8WjzWqYnI0AYOX401JBbKbE4Hsq-bFVi7WrMezipiXt_rE8EdcAC-JW7e7iLYa4UQ12dwq4pansT5lAaJCMBtEY0TL0Ax6OEb2QpF1f05fJdgJJD3r0-zAzDiUtpnP1ToTWaVAVYFYdnGwFjZ3TnTaKCgjhSwTMnj99slUi4wXHTt_BwSRDTbumrqqtNcPWqrcoNDFgIrLshV6ziYnbfEeeRagkzVGlwYO2zFs_9dk com.android.chrome

ra246 Fecha: 2018-07-09 12:12:03 Etiqueta: 000003.log Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Feature Engagement Tracker/AvailabilityDB/000003.log 7433

ra247 Fecha: 2018-07-09 12:12:04 Etiqueta: persisted_profiling_statistics Detalles: filesystem phone/applications0/com.google.android.googlequicksearchbox/backup/f/persisted_profiling_statistics 1341

ra248 Fecha: 2018-07-09 12:12:04 Etiqueta: SearchSettings.bin Detalles: filesystem phone/applications0/com.google.android.googlequicksearchbox/backup/r/app_shared_prefs/SearchSettings.bin 132914

ra249 Fecha: 2018-07-09 12:12:04 Etiqueta: organizacion de proyectos - Buscar con Google Detalles: false https://www.google.com.ec/search?q=organizacion+de+proyectos&oq=organizacion+de+proyectos&aqs=chrome..69i57.7650j0j1&client=ms-android-samsung&sourceid=chrome-mobile&ie=UTF-8 1 com.android.chrome

ra250 Fecha: 2018-07-09 12:12:06 Etiqueta: play.games.ui.sharedPrefs.xml Detalles: filesystem phone/applications0/com.google.android.play.games/backup/sp/play.games.ui.sharedPrefs.xml 1538

ra251 Fecha: 2018-07-09 12:12:08 Etiqueta: com.google.android.apps.chrome.omaha.xml Detalles: filesystem phone/applications0/com.android.chrome/backup/sp/com.google.android.apps.chrome.omaha.xml 695

ra252 Fecha: 2018-07-09 12:12:10 Etiqueta: SIDCC Detalles: false .google.com / AEfoLebYOUpxGnHk3xnCuk-6Zy2PXxznMDj4Iv6BB2rUn8Vn8DDikolWW39CuVviV_IpW2AI com.android.chrome

ra253 Fecha: 2018-07-09 12:12:10 Etiqueta: SIDCC Detalles: false .google.com / AEfoLebYOUpxGnHk3xnCuk-6Zy2PXxznMDj4Iv6BB2rUn8Vn8DDikolWW39CuVviV_IpW2AI com.android.chrome

ra254 Fecha: 2018-07-09 12:12:11 Etiqueta: BrowserMetrics-spare.pma Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/BrowserMetrics-spare.pma 8388608

ra255 Fecha: 2018-07-09 12:12:12 Etiqueta: organizacion de proyectos - Buscar con Google Detalles: false https://www.google.com.ec/search?q=organizacion+de+proyectos&client=ms-android-samsung&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjA0oSezKHcAhVow1kKHXVeA0cQ_AUICCgB&biw=320&bih=452 1 com.android.chrome

ra256 Fecha: 2018-07-09 12:12:22 Etiqueta: Detalles: false https://www.google.com.ec/search?q=organizacion+de+proyectos&client=ms-android-samsung&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjA0oSezKHcAhVow1kKHXVeA0cQ_AUICCgB&biw=320&bih=452#imgrc=BwgJIffsTOe0IM%3A 1 com.android.chrome

ra257 Fecha: 2018-07-09 12:12:29 Etiqueta: Detalles: false https://www.google.com.ec/search?q=organizacion+de+proyectos&client=ms-android-samsung&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjA0oSezKHcAhVow1kKHXVeA0cQ_AUICCgB&biw=320&bih=452#imgrc=aMiFeSxm-Vo5jM%3A 1 com.android.chrome

ra258 Fecha: 2018-07-09 12:12:30 Etiqueta: Visited Links Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Visited Links 131072

ra259 Fecha: 2018-07-09 12:12:30 Etiqueta: Web Data Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Web Data 360448

ra260 Fecha: 2018-07-09 12:12:30 Etiqueta: Web Data-journal Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Web Data-journal 0

ra261 Fecha: 2018-07-09 12:12:30 Etiqueta: 794f39493f83e610_0 Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/GPUCache/794f39493f83e610_0 1484

ra262 Fecha: 2018-07-09 12:12:30 Etiqueta: tab1000 Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_tabs/0/tab1000 106019

ra263 Fecha: 2018-07-09 12:12:30 Etiqueta: tab_state0 Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_tabs/0/tab_state0 422

ra264 Fecha: 2018-07-09 12:12:30 Etiqueta: Detalles: false https://www.google.com.ec/search?q=organizacion+de+proyectos&client=ms-android-samsung&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjA0oSezKHcAhVow1kKHXVeA0cQ_AUICCgB&biw=320&bih=452#imgrc=Q8Wpv7HWxASeqM%3A 1 com.android.chrome

ra265 Fecha: 2018-07-09 12:12:31 Etiqueta: TransportSecurity Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/TransportSecurity 27714

ra266 Fecha: 2018-07-09 12:12:31 Etiqueta: 1P_JAR Detalles: false .google.com.ec / 2018-07-15-17 com.android.chrome

ra267 Fecha: 2018-07-09 12:12:31 Etiqueta: 1P_JAR Detalles: false .google.com.ec / 2018-07-15-17 com.android.chrome

ra268 Fecha: 2018-07-09 12:12:32 Etiqueta: Cookies Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Cookies 425984

ra269 Fecha: 2018-07-09 12:12:32 Etiqueta: Cookies-journal Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Cookies-journal 0

ra270 Fecha: 2018-07-09 12:12:35 Etiqueta: Local StateDetalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Local State 21954

ra271 Fecha: 2018-07-09 12:12:36 Etiqueta: the-real-index Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/GPUCache/index-dir/the-real-index 1416

ra272 Fecha: 2018-07-09 12:12:36 Etiqueta: LOG Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Local Storage/leveldb/LOG 188

ra273 Fecha: 2018-07-09 12:12:39 Etiqueta: Favicons Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Favicons 229376

ra274 Fecha: 2018-07-09 12:12:39 Etiqueta: Favicons-journal Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Favicons-journal 0

ra275 Fecha: 2018-07-09 12:12:39 Etiqueta: History Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/History 196608

ra276 Fecha: 2018-07-09 12:12:40 Etiqueta: the-real-index Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/ShaderCache/GPUCache/index-dir/the-real-index 1392

ra277 Fecha: 2018-07-09 12:12:49 Etiqueta: com.sec.android.gallery3d_preferences.xml Detalles: filesystem phone/applications0/com.sec.android.gallery3d/backup/sp/com.sec.android.gallery3d_preferences.xml 450

ra278 Fecha: 2018-07-09 12:13:01 Etiqueta: History-journal Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/History-journal 8720

ra279 Fecha: 2018-07-09 12:13:45 Etiqueta: google_conversion_tracking.db-journal Detalles: filesystem phone/applications0/com.google.android.youtube/backup/db/google_conversion_tracking.db-journal 21032

ra280 Fecha: 2018-07-09 12:13:45 Etiqueta: youtube.xml Detalles: filesystem phone/applications0/com.google.android.youtube/backup/sp/youtube.xml 58977

ra281 Fecha: 2018-07-09 12:13:50 Etiqueta: google_conversion_tracking.db Detalles: filesystem phone/applications0/com.google.android.youtube/backup/db/google_conversion_tracking.db 20480

ra282 Fecha: 2018-07-09 12:13:55 Etiqueta: dbcom.google.android.libraries.youtube.net.delayedevents.DelayedEventStore Detalles: filesystem phone/applications0/com.google.android.youtube/backup/dbcom.google.android.libraries.youtube.net.delayedevents.DelayedEventStore 20480

ra283 Fecha: 2018-07-09 12:13:55 Etiqueta: dbcom.google.android.libraries.youtube.net.delayedevents.DelayedEventStore-journal Detalles: filesystem phone/applications0/com.google.android.youtube/backup/dbcom.google.android.libraries.youtube.net.delayedevents.DelayedEventStore-journal 82592

ra284 Fecha: 2018-07-09 12:15:33 Etiqueta: Network Persistent State Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Network Persistent State 7224

ra285 Fecha: 2018-07-09 12:16:36 Etiqueta: downloads.db Detalles: filesystem phone/applications0/com.android.providers.downloads/backup/db/downloads.db 114688

ra286 Fecha: 2018-07-09 12:16:36 Etiqueta: Maps: Navegación y tránsito Detalles: false application/vnd.android.package-delta com.android.vending https://play.googleapis.com/download/by-token/download?token=AOTCm0TDjGeOLus5RQvJI4U_-gclogulZG1wjNoJlNlVEOL-RhKMhqf2wYD0e77O4go0Ty0bPL4YSFWF_bSaCwT6NUGyVus3FRZxjR-JZWsr9Q31GN0N0Bp7l_Vurar-z3bGD73i4E9GBIof92L6lIc4CnFuBWIeDUlbmIXVwFScqg8C49sYwdUIZ1zO0Kd6C-2LGD_CmhexYq89J9buRP6YIjm4br-FZHWU-nUKhOX1OtgBYdOYYgI_72OSYK6pfVAK1F0eKizwX8IDfJG22z5YU31mHjm0KPmG3gSPVWXyf5gVLOTPMYbBKyDy_eyQEtssp_yBZGhijREwTBVxNAKjFd3zS-s8Pr0Mt_Wy_BF5dSbMwoc&cpn=AwP3oKwmjIUjPe8D&isid=QJxAf8g-QOa1kef4S8gb1Q

ra287 Fecha: 2018-07-09 12:16:38 Etiqueta: badge.db Detalles: filesystem phone/applications0/com.sec.android.provider.badge/backup/db/badge.db 20480

ra288 Fecha: 2018-07-09 12:19:01 Etiqueta: com.android.chrome_preferences.xml Detalles: filesystem phone/applications0/com.android.chrome/backup/sp/com.android.chrome_preferences.xml 8246

ra289 Fecha: 2018-07-09 12:21:19 Etiqueta: external.db-wal Detalles: filesystem phone/applications0/com.android.providers.media/backup/db/external.db-wal 4297192

ra290 Fecha: 2018-07-09 12:25:33 Etiqueta: DATA_Preferences Detalles: filesystem phone/applications0/com.sec.android.gallery3d/backup/f/DATA_Preferences 2000

ra291 Fecha: 2018-07-09 12:25:33 Etiqueta: lastest_view_state.xml Detalles: filesystem phone/applications0/com.sec.android.gallery3d/backup/sp/lastest_view_state.xml 119

ra292 Fecha: 2018-07-09 12:27:31 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.android.providers.partnerbookmarks/backup/_manifest 2533

ra293 Fecha: 2018-07-09 12:27:31 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.sec.android.app.ringtoneBR/backup/_manifest 2525

ra294 Fecha: 2018-07-09 12:27:32 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.android.contacts/backup/_manifest 2515

ra295 Fecha: 2018-07-09 12:27:32 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.android.htmlviewer/backup/_manifest 2517

ra296 Fecha: 2018-07-09 12:27:32 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.google.android.gsf.login/backup/_manifest 2233

ra297 Fecha: 2018-07-09 12:27:32 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.sec.android.fotaclient/backup/_manifest 2520

ra298 Fecha: 2018-07-09 12:27:32 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.sec.android.gallery3d/backup/_manifest 2520

ra299 Fecha: 2018-07-09 12:27:33 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.android.calendar/backup/_manifest 2515

ra300 Fecha: 2018-07-09 12:27:33 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.android.documentsui/backup/_manifest 2518

ra301 Fecha: 2018-07-09 12:27:33 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.android.providers.calendar/backup/_manifest 2525

ra302 Fecha: 2018-07-09 12:27:33 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.android.providers.downloads.ui/backup/_manifest 2529

ra303 Fecha: 2018-07-09 12:27:33 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.sec.android.allshare.service.fileshare/backup/_manifest 2537

ra304 Fecha: 2018-07-09 12:27:33 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.sec.android.app.sbrowser/backup/_manifest 2530

ra305 Fecha: 2018-07-09 12:27:33 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.sec.android.provider.badge/backup/_manifest 2524

ra306 Fecha: 2018-07-09 12:27:34 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.android.mms/backup/_manifest 2510

ra307 Fecha: 2018-07-09 12:27:34 Etiqueta: external.db-shm Detalles: filesystem phone/applications0/com.android.providers.media/backup/db/external.db-shm 32768

ra308 Fecha: 2018-07-09 12:27:35 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.android.providers.media/backup/_manifest 2523

ra309 Fecha: 2018-07-09 12:27:38 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.android.dreams.phototable/backup/_manifest 2524

ra310 Fecha: 2018-07-09 12:27:38 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.google.android.marvin.talkback/backup/_manifest 1284

ra311 Fecha: 2018-07-09 12:27:38 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.google.android.setupwizard/backup/_manifest 2236

ra312 Fecha: 2018-07-09 12:27:38 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.google.android.street/backup/_manifest 2233

ra313 Fecha: 2018-07-09 12:27:38 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.monotype.android.font.rosemary/backup/_manifest 2528

ra314 Fecha: 2018-07-09 12:27:38 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.monotype.android.font.samsungsans/backup/_manifest 2531

ra315 Fecha: 2018-07-09 12:27:38 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.samsung.video/backup/_manifest 2520

ra316 Fecha: 2018-07-09 12:27:38 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.sec.android.app.chromecustomizations/backup/_manifest 2534

ra317 Fecha: 2018-07-09 12:27:38 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.sec.android.widgetapp.webmanual/backup/_manifest 2529

ra318 Fecha: 2018-07-09 12:27:39 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.google.android.googlequicksearchbox/backup/_manifest 2270

ra319 Fecha: 2018-07-09 12:27:39 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.sec.android.pagebuddynotisvc/backup/_manifest2535

ra320 Fecha: 2018-07-09 12:28:15 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.android.exchange/backup/_manifest 2520

ra321 Fecha: 2018-07-09 12:28:15 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.android.wallpaper.livepicker/backup/_manifest 2527

ra322 Fecha: 2018-07-09 12:28:15 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.google.android.backuptransport/backup/_manifest 2239

ra323 Fecha: 2018-07-09 12:28:15 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.sec.android.providers.tasks/backup/_manifest 2526

ra324 Fecha: 2018-07-09 12:28:15 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.sec.android.widgetapp.ap.hero.accuweather/backup/_manifest 2539

ra325 Fecha: 2018-07-09 12:28:16 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.android.email/backup/_manifest 2517

ra326 Fecha: 2018-07-09 12:28:16 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.compelson.migrator/backup/_manifest 1868

ra327 Fecha: 2018-07-09 12:28:16 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.google.android.apps.maps/backup/_manifest 2240

ra328 Fecha: 2018-07-09 12:28:16 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.sec.android.splitsound/backup/_manifest 2520

ra329 Fecha: 2018-07-09 12:28:16 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.sec.enterprise.knox.cloudmdm.smdms/backup/_manifest 2533

ra330 Fecha: 2018-07-09 12:28:45 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.android.providers.settings/backup/_manifest 2525

ra331 Fecha: 2018-07-09 12:28:45 Etiqueta: flattened-data Detalles: filesystem phone/applications0/com.android.providers.settings/backup/f/flattened-data 2312

ra332 Fecha: 2018-07-09 12:28:45 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.android.wallpapercropper/backup/_manifest 2523

ra333 Fecha: 2018-07-09 12:28:45 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.google.android.apps.docs/backup/_manifest 2259

ra334 Fecha: 2018-07-09 12:28:45 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.sec.android.app.FileShareClient/backup/_manifest 2530

ra335 Fecha: 2018-07-09 12:28:49 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.android.browser.provider/backup/_manifest 2523

ra336 Fecha: 2018-07-09 12:28:49 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.android.providers.downloads/backup/_manifest 2526

ra337 Fecha: 2018-07-09 12:28:49 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.google.android.videos/backup/_manifest 1239

ra338 Fecha: 2018-07-09 12:28:49 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.percent.bbtanroulette/backup/_manifest 1497

ra339 Fecha: 2018-07-09 12:28:49 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.samsung.android.app.accesscontrol/backup/_manifest 2531

ra340 Fecha: 2018-07-09 12:28:49 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.samsung.safetyinformation/backup/_manifest 2523

ra341 Fecha: 2018-07-09 12:28:50 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.android.proxyhandler/backup/_manifest 2519

ra342 Fecha: 2018-07-09 12:28:50 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.google.android.feedback/backup/_manifest 2232

ra343 Fecha: 2018-07-09 12:28:50 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.google.android.onetimeinitializer/backup/_manifest 2242

ra344 Fecha: 2018-07-09 12:28:50 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.google.android.talk/backup/_manifest 2234

ra345 Fecha: 2018-07-09 12:28:50 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.monotype.android.font.cooljazz/backup/_manifest 2528

ra346 Fecha: 2018-07-09 12:28:50 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.sec.android.app.fm/backup/_manifest 2516

ra347 Fecha: 2018-07-09 12:28:50 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.sec.android.provider.logsprovider/backup/_manifest 2531

ra348 Fecha: 2018-07-09 12:28:51 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.android.pacprocessor/backup/_manifest 2519

ra349 Fecha: 2018-07-09 12:28:51 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.android.providers.userdictionary/backup/_manifest 2531

ra350 Fecha: 2018-07-09 12:28:51 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.osp.app.signin/backup/_manifest 943

ra351 Fecha: 2018-07-09 12:28:51 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.sec.android.app.FileShareServer/backup/_manifest 2530

ra352 Fecha: 2018-07-09 12:28:51 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.sec.android.app.myfiles/backup/_manifest 2521

ra353 Fecha: 2018-07-09 12:28:51 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.sec.android.app.popupcalculator/backup/_manifest 2537

ra354 Fecha: 2018-07-09 12:28:51 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.sec.enterprise.mdm.vpn/backup/_manifest 2521

ra355 Fecha: 2018-07-09 12:28:51 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.sec.smartcard.manager/backup/_manifest 2519

ra356 Fecha: 2018-07-09 12:28:52 Etiqueta: _manifest Detalles: filesystem phone/applications0/android/backup/_manifest 2502

ra357 Fecha: 2018-07-09 12:28:52 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.android.dreams.basic/backup/_manifest 2519

ra358 Fecha: 2018-07-09 12:28:52 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.android.externalstorage/backup/_manifest 2522

ra359 Fecha: 2018-07-09 12:28:52 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.google.android.syncadapters.calendar/backup/_manifest 2245

ra360 Fecha: 2018-07-09 12:28:52 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.samsung.android.sdk.spenv10/backup/_manifest 903

ra361 Fecha: 2018-07-09 12:28:52 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.sec.android.app.samsungapps/backup/_manifest 1227

ra362 Fecha: 2018-07-09 12:28:52 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.sec.android.app.soundalive/backup/_manifest 2533

ra363 Fecha: 2018-07-09 12:28:52 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.sec.android.provider.emergencymode/backup/_manifest 2532

ra364 Fecha: 2018-07-09 12:28:52 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.sec.android.widgetapp.SPlannerAppWidget/backup/_manifest 2537

ra365 Fecha: 2018-07-09 12:28:53 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.android.vending/backup/_manifest 2249

ra366 Fecha: 2018-07-09 12:29:01 Etiqueta: Preferences Detalles: filesystem phone/applications0/com.android.chrome/backup/r/app_chrome/Default/Preferences 34345

ra367 Fecha: 2018-07-09 12:29:01 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.google.android.play.games/backup/_manifest 2259

ra368 Fecha: 2018-07-09 12:29:01 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.sec.android.app.clockpackage/backup/_manifest 2526

ra369 Fecha: 2018-07-09 12:29:01 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.sec.android.app.videoplayer/backup/_manifest 2525

ra370 Fecha: 2018-07-09 12:29:02 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.riseup.game/backup/_manifest 2887

ra371 Fecha: 2018-07-09 12:29:09 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.google.android.gm/backup/_manifest 2251

ra372 Fecha: 2018-07-09 12:29:17 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.google.android.youtube/backup/_manifest 1264

ra373 Fecha: 2018-07-09 12:29:17 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.sec.android.mmapp/backup/_manifest 2515

ra374 Fecha: 2018-07-09 12:29:17 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.sec.android.widgetapp.dualclockdigital/backup/_manifest 2536

ra375 Fecha: 2018-07-09 12:29:32 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.google.android.apps.magazines/backup/_manifest 2265

ra376 Fecha: 2018-07-09 12:29:38 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.android.chrome/backup/_manifest 2249

ra377 Fecha: 2018-07-09 12:29:38 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.android.keyguard/backup/_manifest 2515

ra378 Fecha: 2018-07-09 12:29:38 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.samsung.klmsagent/backup/_manifest 2515

ra379 Fecha: 2018-07-09 12:29:38 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.wsomacp/backup/_manifest 2512

ra380 Fecha: 2018-07-09 12:29:48 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.google.android.syncadapters.contacts/backup/_manifest 2245

ra381 Fecha: 2018-07-09 12:29:48 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.monotype.android.font.chococooky/backup/_manifest 2530

ra382 Fecha: 2018-07-09 12:29:48 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.sec.android.app.voicerecorder/backup/_manifest2535

ra383 Fecha: 2018-07-09 12:29:48 Etiqueta: _manifest Detalles: filesystem phone/applications0/com.sec.esdk.elm/backup/_manifest 2510

Apéndice C

Formato de Informe Pericial

Este apéndice, se presentan el formato que se debe seguir según el Consejo de la Judicatura.

C.1. DATOS GENERALES DEL JUICIO, O PROCESO DE INDAGACIÓN PREVIA

Nombre Judicatura o Fiscalía:.....
No. de Proceso: 00000001.....
Nombre y Apellido de la o el Perito: Jessica Paola Camacho Cajamarca
Profesión y Especialidad acreditada: Ingeniería Electrónica y Telecomunicaciones
No. de Calificación: 123456
Dirección de Contacto: San Francisco - Azogues - Cañar
Teléfono fijo de contacto: 07-2243139.....
Teléfono celular de contacto: 0987935551.....
Correo electrónico de contacto: jessica.camachoc@gmail.com.....
Fecha(DD/MM/AAAA) de incautación: 09/07/2018.....Hora: 20:00:00
Lugar y ubicación: Universidad XYZ.....

C.2. PARTE DE ANTECEDENTES

He sido llamada como perito por , doctora abogada de la facultad de Ingeniería de la Universidad XYZ, con cédula de ciudadanía 030183646-6; para entregar un informe técnico pericial con el fin de conocer las actividades realizadas en un dispositivo celular móvil.

C.2.1. Antecedentes

La propuesta en el que se efectúa la investigación es a través de una prueba de concepto, donde se desarrolla un examen forense basándose en el objetivo que aborda la manera de recolectar la información de actividades desarrolladas en el dispositivo celular móvil marca Samsung con sistema operativo Android que será el objetivo de análisis.

C.2.2. Prueba de concepto

Al realizar un examen a los estudiantes de octavo nivel de la asignatura de Organización y Evaluación de Proyectos de la facultad de Ingeniería de la Universidad XYZ, el docente nota

que un estudiante realizó un intento de copia, por lo que se verificó y se descubrió que poseía un dispositivo móvil escondido, por lo que se le pidió al estudiante entregar el examen y retirarse.

El docente solicita incautar el dispositivo para determinar las actividades que realizó durante el examen y de este modo verificar si están relacionadas con el tema de la asignatura y solicitar que se desarrolle una investigación de las actividades que realiza el estudiante con dicho teléfono, debido a la sospecha de una posible copia.

C.2.3. Alcance

- Determinar las actividades como: historial de navegación, descargas, llamadas, aplicaciones, mensajes.
- Obtener un registro de las actividades del día 9 de julio de 2018.

C.3. PARTE DE CONSIDERACIONES TÉCNICAS O METODOLOGÍA A APLICARSE

Yo, Srta. Jessica Camacho Cajamarca, con experiencia adquirida en mis años de estudiante universitario en la carrera de Ingeniería de la Universidad de Cuenca en el manejo de tecnologías; que dan fe al correcto cumplimiento del encargo encomendado en orden a efectuar una pericia formulo el siguiente **Diseño de Pericia**, conforme la siguiente pauta de trabajo y desarrollo que determinará los objetivos perseguidos.

Diseño de Pericia:

- Identificación y preservación de los elementos
- Adquisición de todos los datos que contenga el dispositivo móvil con diferentes herramientas.
- Análisis de registro de actividades.

C.4. PARTE DE CONCLUSIONES

Una vez analizados los antecedentes y tomando en base lo especificado en las preguntas respectivas este perito puede concluir lo siguiente:

PREGUNTA:

- Pericia informática respecto a las actividades realizadas por un estudiante en un dispositivo móvil marca Samsung, el día 9 de julio de 2018 entre las 11h00 a 13h00.

CONCLUSIÓN:

Luego del análisis realizado del reporte otorgado por la herramienta RegistroActividades, se concluye que:

- Se encontraron 25 actividades relacionadas con al asignatura Organización y Evaluación de Proyectos, con todas las pruebas dadas es claro que el estudiante realizó plagio en el examen.
- En un lapso de media hora navegó en el explorador web del dispositivo buscando términos asociados a la materia como: planificar las repuestas a los riesgos, interacción entre grupos de procesos en un proyecto, identificación de riegos.
- Se recuperó las 4 imágenes relacionadas al tema de la prueba que había en su teléfono con los siguientes títulos: escala de impacto, escala de probabilidad y riesgos.
- Se verificó el acceso a la aplicación de mensajería instantánea WhatsApp y el mensaje de voz que se envió.
- Se realizó la descarga de un archivo pdf con el siguiente título: Identificación de los riesgos.

Esto de acuerdo a lo solicitado en la pericia.

C.5. PARTE DE INCLUSIÓN DE DOCUMENTOS DE RESPALDO, ANEXOS, O EXPLICACIÓN DE CRITERIO TÉCNICO.

Luego de la investigación de las tecnologías requeridas para atender la solicitud y realizar las pruebas, procedo a presentar mi opinión técnica a cada pregunta formulada al momento de requerir esta pericia.

C.5.1. Fase de identificación y preservación

a. Equipo de investigación

Tabla C.1: Equipo de investigación

Nombre y Apellido	Cargo	Identificación
Jessica Camacho	Custodios	3456899
Priscila Cedillo		3456872
Jessica Camacho	Peritos	3426898
Karina Campos		
Jessica Camacho	Examinador	3435985

b. Materiales

Materiales y equipos para los responsables de la investigación forense.

Tabla C.2: Materiales

Materiales	Acceso	
	SI	NO
Computador	x	
Cámara	x	
Etiquetas	x	
Guantes de látex		x
Cable de datos USB	x	
Cargador del teléfono	x	
Paquete para aislar el dispositivo	x	
Lector de tarjeta SIM		x
Software forense	x	
Lector de memoria externa		x
Dispositivo externo para backup		x
Documentos para registo de actividades	x	

c. Procedimiento

- A solicitud de la secretaria abogada de la facultad, y por petición del docente de la Universidad XYZ se realiza la entrega de un dispositivo celular móvil, las características se detallan en la Tabla C.5 C.6.
- Al estar el teléfono encendido y con el porcentaje de batería mayor al 50 %, se procede a desactivar Wi-Fi, Bluetooth y colocar en modo avión.
- El dispositivo tiene contraseña tipo PIN, para desbloquear el teléfono se acuerda una reunión con el usuario para que proporcione dicha contraseñas.

- El teléfono, cable USB, cargador, SIM y memoria externa incautados se procede a tomar fotografías. Adjunto en un registro visual Figuras C.1, C.2, C.3, C.4.
- Se inicia a etiquetar cada elemento incautado los códigos se detallan en las Tablas C.5, C.6. Se aislar y sella para el empaquetado y transporte.
- Firmas de la entrega de los dispositivos como parte de la solicitud de examen forense.
- Todos dispositivos y periféricos se colocan en una caja de cartón para ser sellados y transportados al laboratorio.

d. Descripción de la evidencia

Tabla C.3: Descripción de la evidencia

Evidencia				
Código etiqueta	Cant.	Estado	Caracteristícas	Periféricos
D001-C001	1	Encendido (x) Apagado ( ) Bloqueado (x)	Sistema Operativo Androi Samsung Carga de batería 68 % Modelo: SM-J11H/DS FCC ID: A3LSMJ110H Carga: 3.8 V -6.84Wh -2600mAH IMEI: 358817/07/293555/9 Pantalla: 4.3 pulgadas Cámara frontal y posterior S/N:RV1H40Z7ROH Wi-Fi Bluetooth Memoria interna 4GB Memoria externa 2GB	Manuales ( ) Cargador (x) Batería (x) SIM (x) Cable USB (x) Memoria externa (x) Otros (x)

e. Aprobación

.....	.....
Sr. Juan Perez	Ing. Karina Campos
Propietario	Perito
.....	.....
Ing. Priscila Cedillo	Sra. Jessica Camacho
Custidio	Analista

f. Registro visual

(a) Cara frontal.

(b) Cara posterior.

Figura C.1: Teléfono celular marca Samsung.

(a) Porcentaje de batería.

(b) Batería.

Figura C.2: Batería de teléfono celular.

(a) Cable USB marca Samsung.

(b) Cargador marca Samsung.

Figura C.3: Cable USB y cargador del teléfono celular.

Figura C.4: Accesorio (estuche).

g. Observaciones

- El dispositivo está en buenas condiciones por lo que no hubo la necesidad de especialistas externo.
- No se adquiere huellas dactilares en este caso debido a que no es un crimen penal.

C.5.2. Fase de adquisición

a. Descripción de las herramientas

Se procede a emplear varias herramientas forenses debido a que con un sólo software no se puede extraer la totalidad de la información, en ciertos casos una sola aplicación de *software* da

la extracción de información de mensajes, llamadas y agenda, otro software da la información de imágenes y videos. Por lo tanto, para un perito es necesario utilizar varias herramientas y tener la evidencia completa.

Tabla C.4: Descripción de herramientas

Herramienta	Descripción
SDK de Android	Acceso al dispositivo por medio de ADB.
MD5summer hashdeep	Verificar integridad de datos mediante hash.
Andriller MOBILedit Oxygen Forensic	Herramienta forense tipo comercial para la extracción y análisis de información.
Autopsy Bulk_extractor Kali Linux	Herramientas forenses de código abierto para las extracción y análisis de información.
Registro de actividades	Herramienta que proporciona un registro de actividades

b. Procedimiento

- Desempaquetar la evidencia comprobando que no hubo ningún daño, caso contrario colocar en observaciones.
- Comprobar el nivel de batería del dispositivo, como es superior al 50 % no cargar el móvil.
- Conectar el teléfono mediante le cable de datos USB al computador.
- Colocar en modo depuración: Desbloquear el dispositivo - Configuraciones - Ajustes - Opciones de desarrollador - Depuración de USB.
- Realizar el *backup* del dispositivo mediante cable de datos USB.
  - Mediante comando de consola ADB
  - Se ingresa en consola *adb devices* para comprobar que el teléfono este conectado.

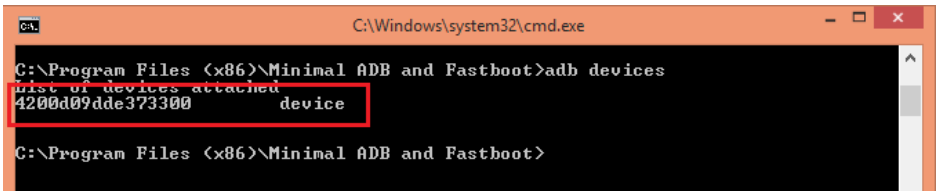


Figura C.5: Dispositivo móvil conectado.

- Se ingresa *adb shell getprop* para conocer las características del dispositivo.

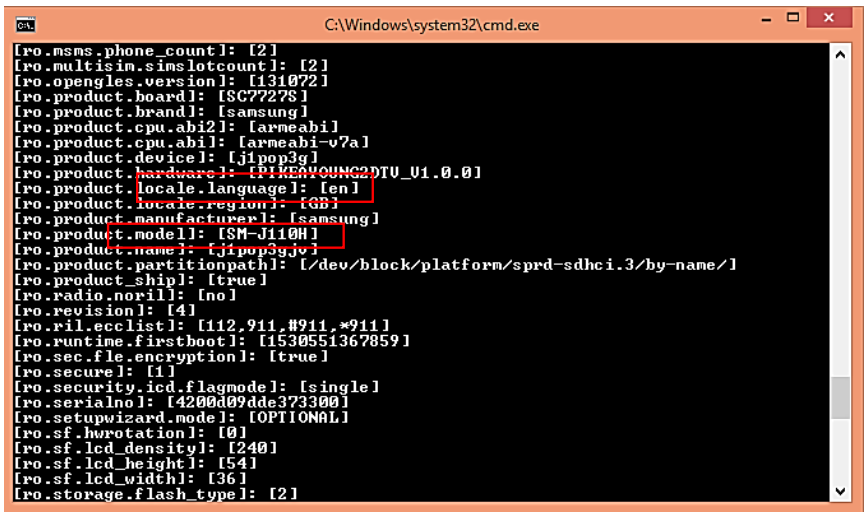


Figura C.6: Características del dispositivo móvil..

- Se realiza el backup *-f C:/backup0001/SM-J110H/nombredecadaelementocopiado.ab -apk -shared -all -system*

- Asegurar la copia, no es necesario ingresar una contraseña.
- Iniciar el backup.

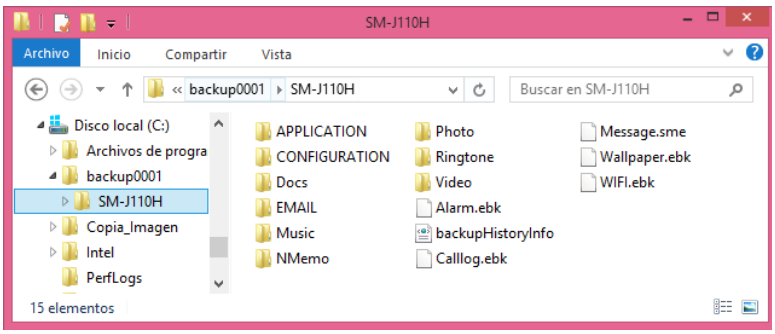


Figura C.7: Backup del teléfono marca Samsung

- Obtener hash mediante MD5Summer.

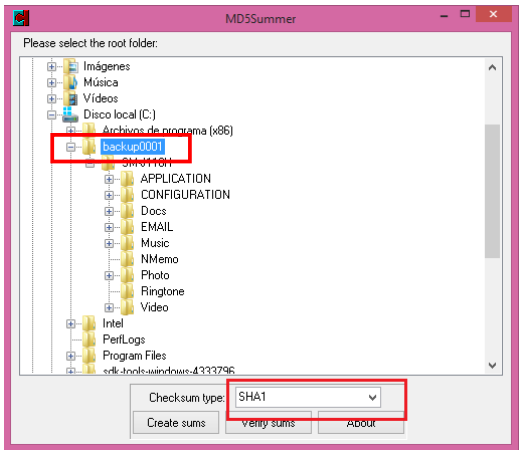


Figura C.8: Selección de la carpeta y el tipo de *hash*.

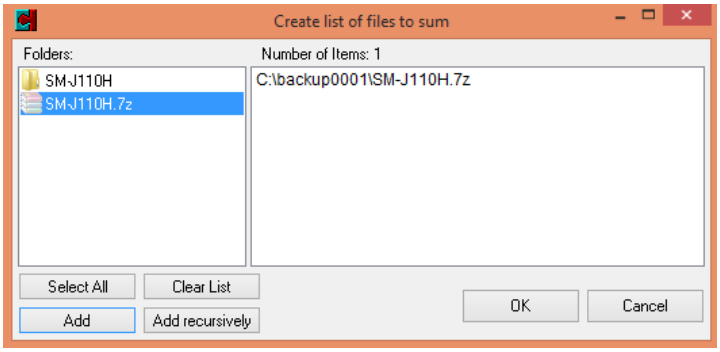


Figura C.9: Creación de *hash* MD5Summer.

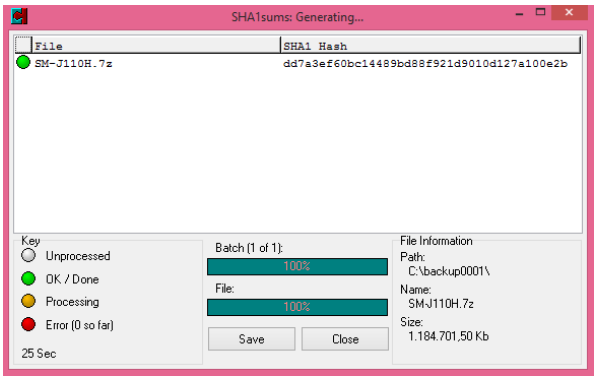


Figura C.10: Generación y guardado *hash* con sha1 MD5Summer.

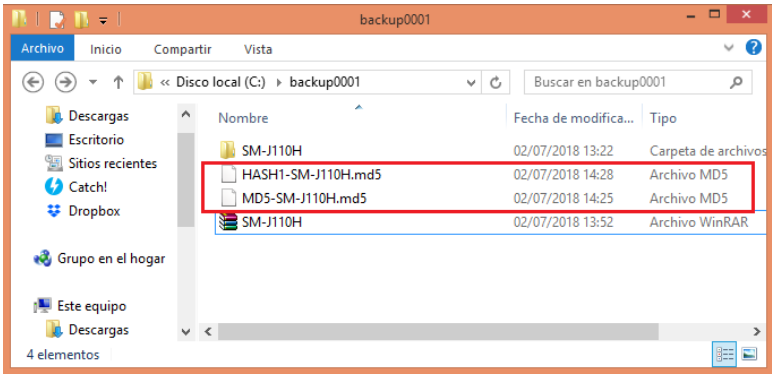


Figura C.11: Archivos *hash* MD5Summer.

- Obtener imagen forense mediante las herramientas Andriller, MOBILedit y Oxygen forensic.

  - La imagen extraída de cada herramienta se guarda en *-f C:/Copia imagen/nombreherramienta*

Imagen obtenida de Andriller

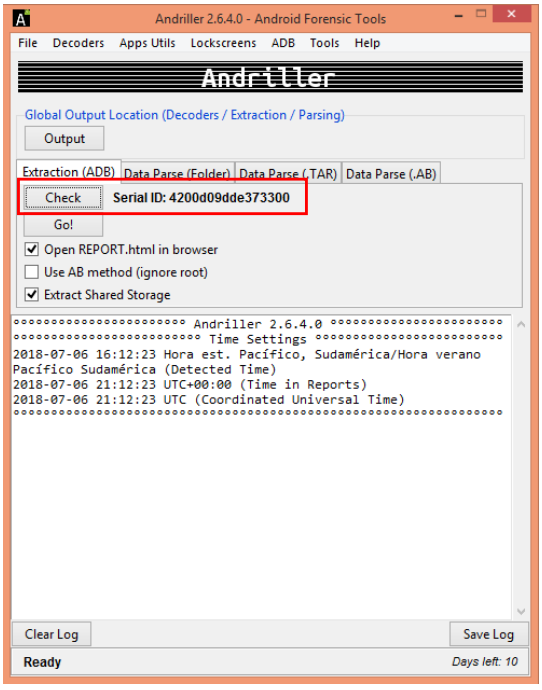


Figura C.12: Se verifica que el dispositivo esté conectado.

Figura C.13: Se ingresar la ruta donde se guarda la imagen.

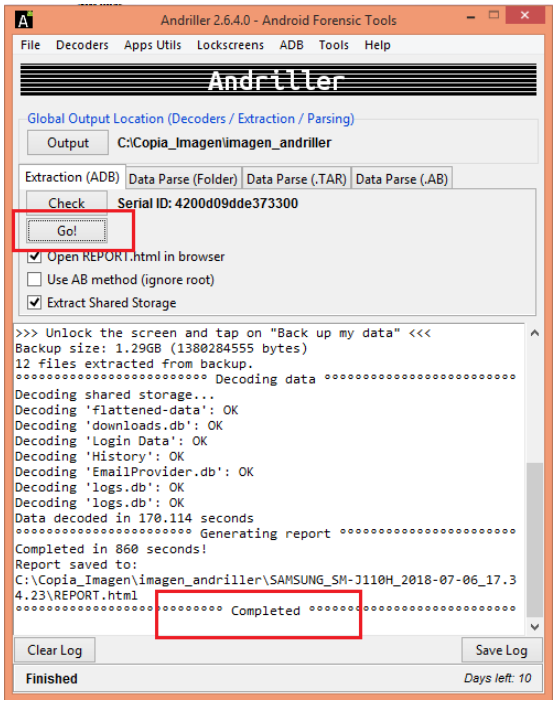


Figura C.14: Iniciación el proceso.

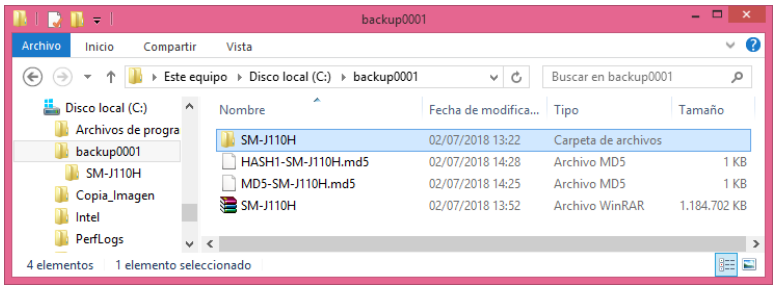


Figura C.15: Carpeta con los archivos extraídos.

Imagen obtenida de MOBILedit

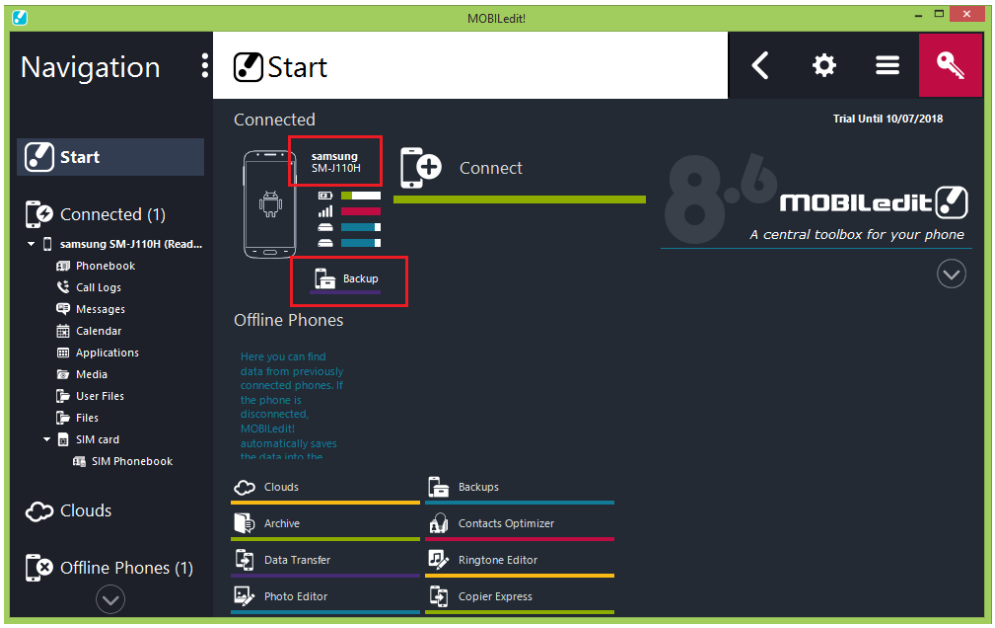


Figura C.16: Iniciación la conexión con MOBILedit e iniciar la copia de seguridad.

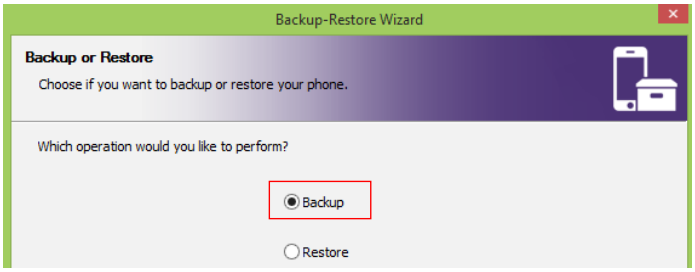


Figura C.17: Se escoge la opción Backup.

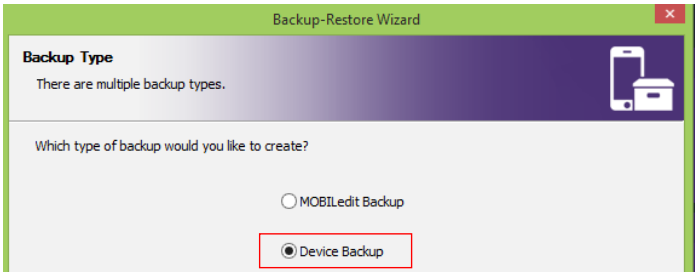


Figura C.18: Se escoge Device Backup.

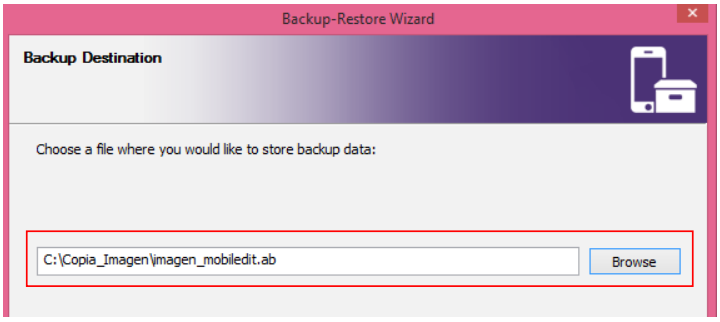


Figura C.19: Se escoge la ruta donde se va a guardar la copia.

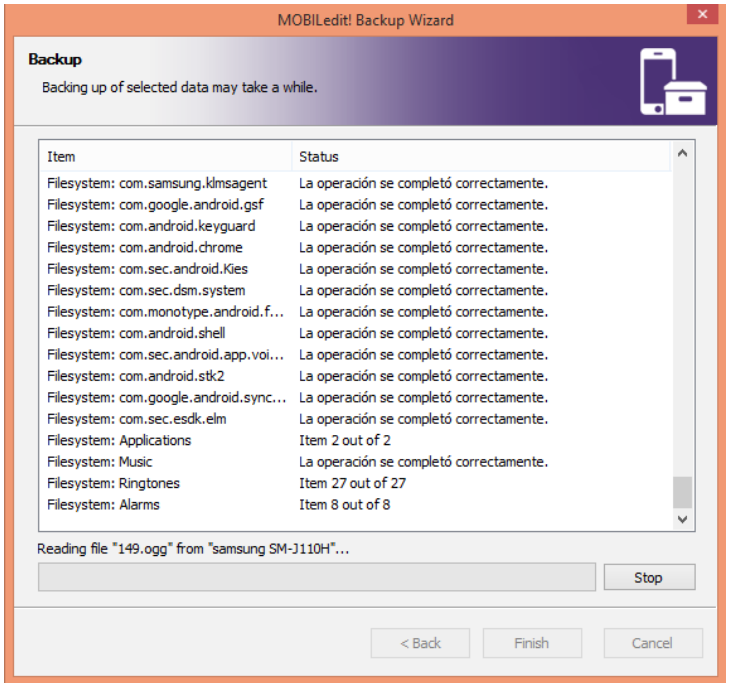


Figura C.20: Se inicia la extracción de datos.

Imagen obtenida de Oxygen Forensic

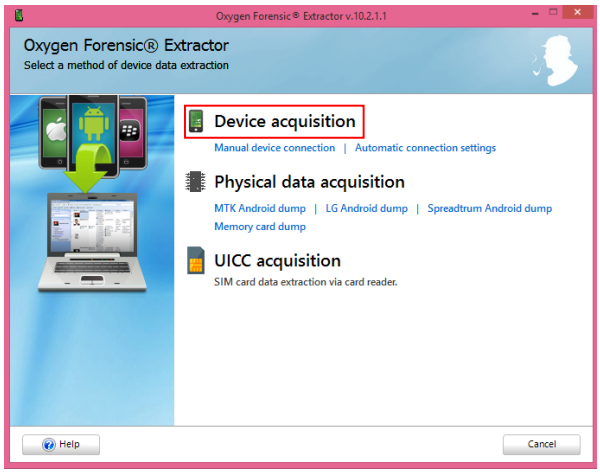


Figura C.21: Conexión del dispositivo a Oxygen Forensic (opción *Device acquisition*).

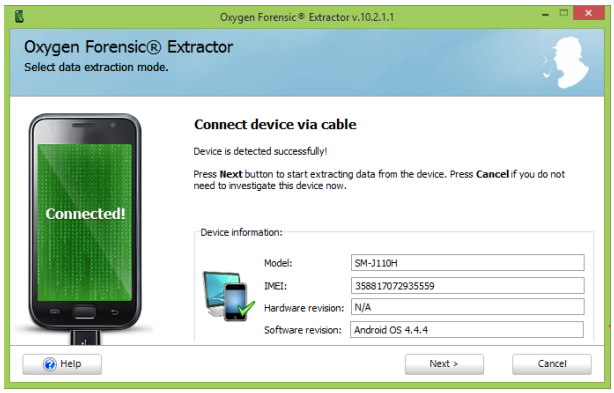


Figura C.22: Presentación de los datos del dispositivo.

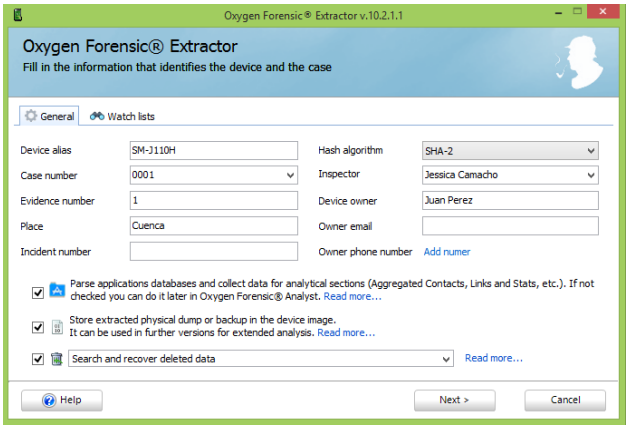


Figura C.23: Se ingresa los datos del caso.

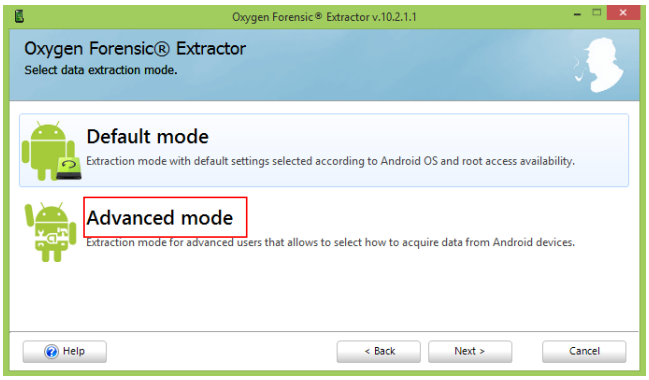


Figura C.24: Selección el modo de extracción.

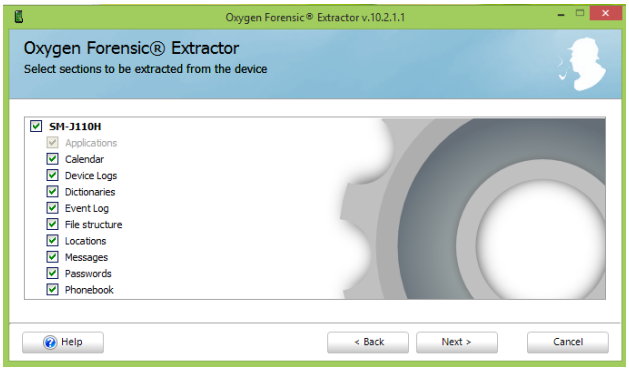


Figura C.25: Selección la información que se va extraer.

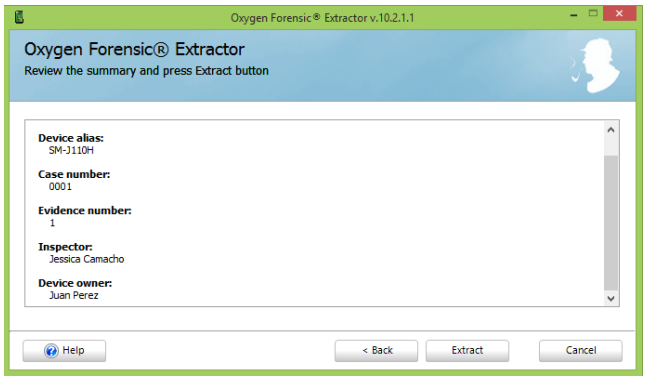


Figura C.26: Iniciar el proceso de extracción.

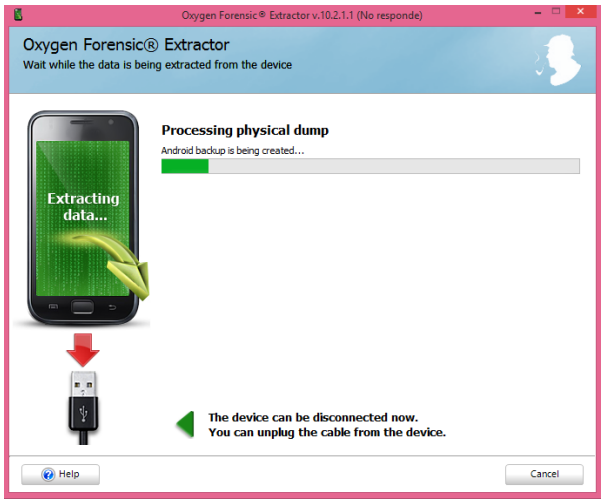


Figura C.27: Inicio del proceso de extracción de la información.

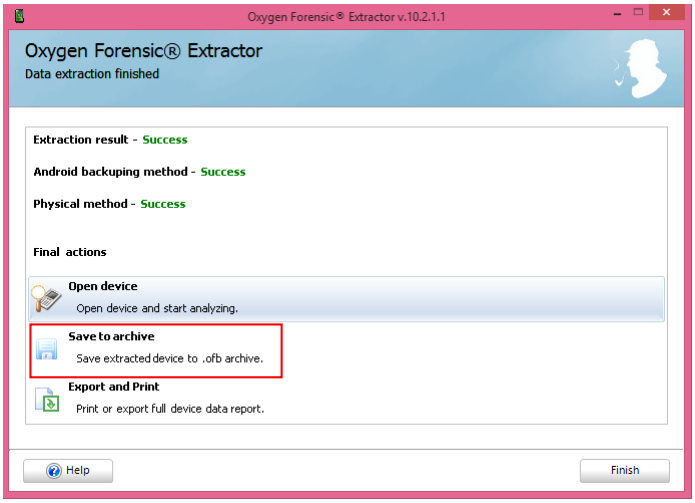


Figura C.28: Extracción finalizada y almacenamiento de la información.

c. Información del dispositivo incautado

Tabla C.5: Características de teléfono

Dispositivo		
Etiqueta dispositivo:	D001-C001	
Tipo de dispositivo:	Teléfono celular	
Propietario:	Juan Perez	
Marca:	Samsung Galaxy	
Modelo:	SM-J110H/DS	
Estado:	Encendido (x)	Apagado ( )
Características Físicas		
Procesador:	1.3 GHz Dual Core	
Pantalla:	109.2 mm (4.3 pulgadas) WVGA	
Cámara:	5MP AF+ 2MP	
FCC ID:	A3LSMJ110H	
IMEI:	358817/07/293555/9	
SSN:	J110H/DSGSMH	
S/N:	RV1H40Z7R0H	
Interfaz de conexión:	USB	
Tarjeta externa:	SI ( )	NO (x)
SIM:	SI (x)	NO ( )
Características Lógicas		
Sistema Operativo:	Android	
Versión:	4.4.1	
Idioma:	Español	
Almacenamiento interno:	4GB	
Modo avión:	SI (x)	NO ( )
Conexión inalámbrica		
Bluetooth:	SI (x)	NO ( )
Wi-Fi:	SI (x)	NO ( )
Infrarrojo:	SI (x)	NO (x)
Batería		
Extraible:	SI(x)	NO( )
Nivel (%):	68 %	
Marca:	Samsung	
Características:	EB-BJ111ABE	
S/N:	LC1H4104S/2-B	
Características:	3.8V -6.84 Wh - 2600 mAh	
Etiqueta:	DB0001	

Tabla C.6: Características de otros dispositivos

Memoria Extraible	
Marca:	Kingston
Características:	SD-CO2G
Capacidad:	2GB
Etiqueta:	MEX0001
Cargador	
Marca:	Samsung
Modelo:	EP-TA50JWE
Etiqueta:	DCAR0001
Cable de Datos	
Marca:	Samsung
Etiqueta:	CDAT0001

d. Observaciones

- Por ser un caso de estudio, no se obtiene acceso root al teléfono, debido a que en este proceso el teléfono debe ser apagado o en casos extremos daño del mismo.

C.5.3. Fase de análisis

a. Extracción de información

- Adquirir reporte de la herramienta Andriller. Al obtener la imagen forense Andriller paralelamente genera un reporte en formato HTML y Excel.

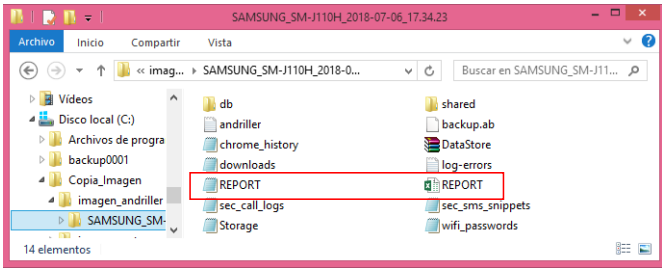


Figura C.29: Reporte generado por Andriller.

- Obtener el reporte de la herramienta Oxygen Forensic. El reporte se guarda en la ruta -f C:/Copia_Imagen/imagen_oxygen.

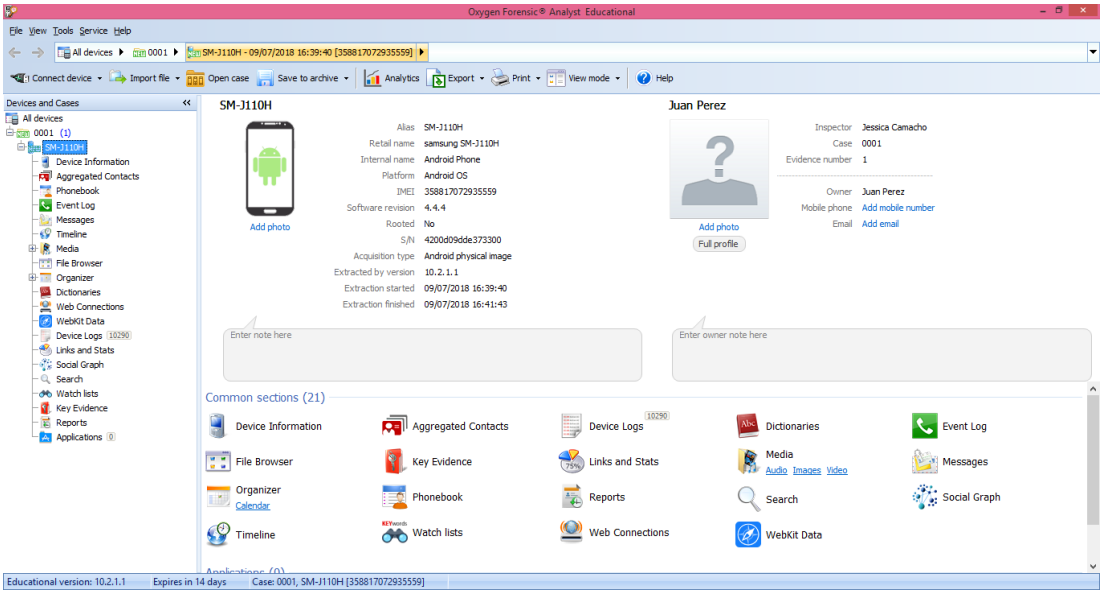


Figura C.30: Información del dispositivo.

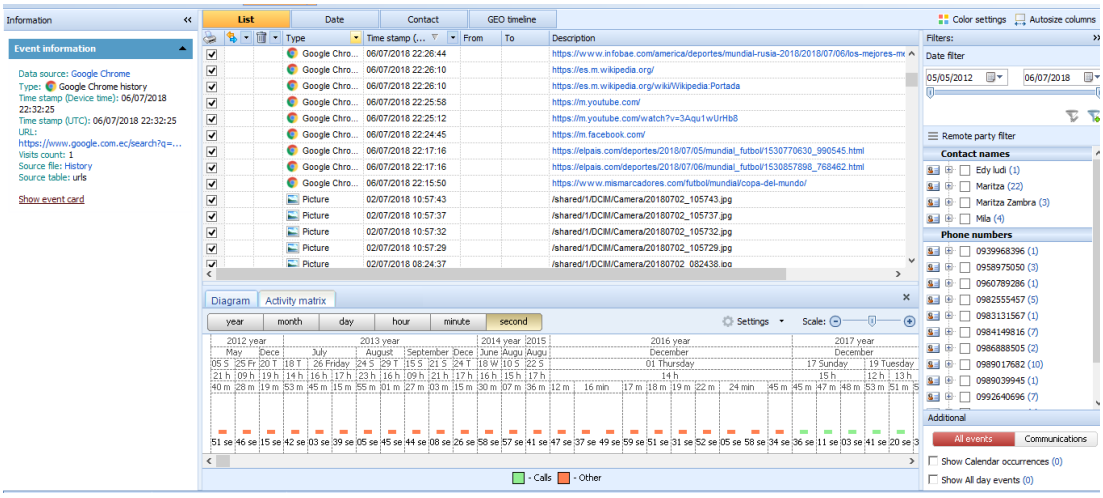


Figura C.31: Se escoger las carpetas con la información que va a presentar en el reporte y se exporta los archivos.

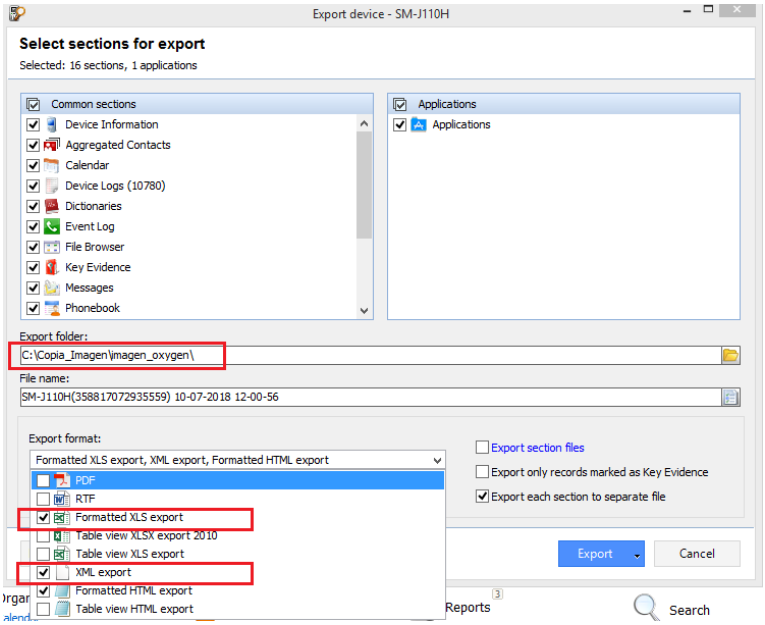


Figura C.32: Se escoge la ruta donde se va a guardar y el formato del reporte que se va exportar.

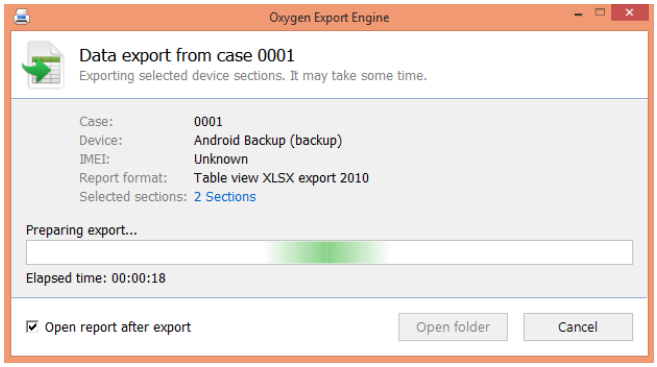


Figura C.33: Se inicia la exportación de los archivos.

- Obtener el reporte de la herramienta MOBILedit. El reporte se guarda en la ruta -f C:/Copia_Imagen/imagen_mobiledit.

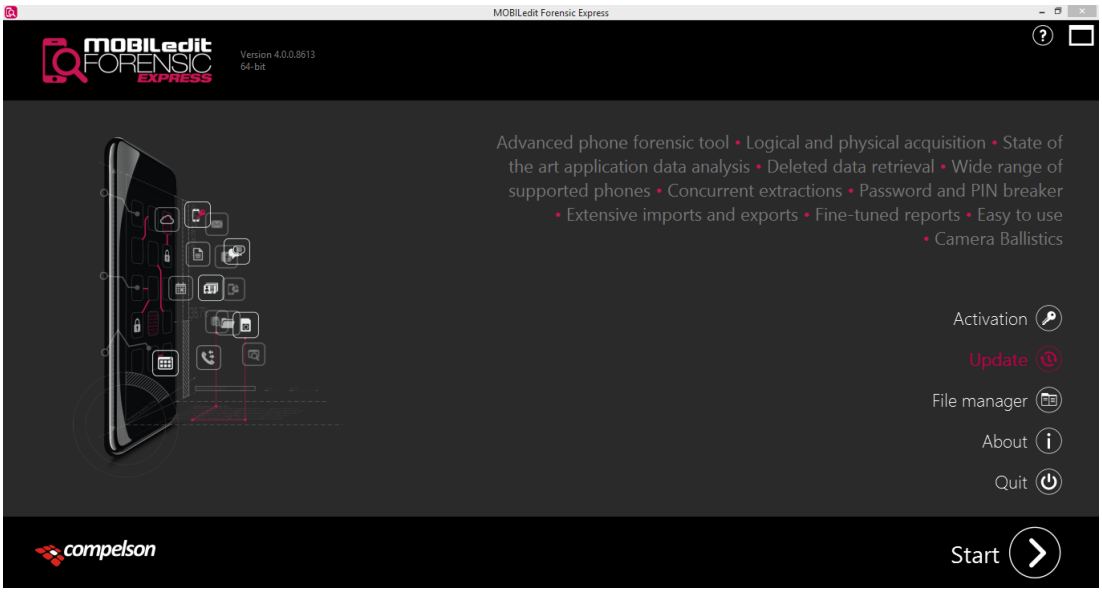


Figura C.34: Se inicia el proceso pulsando el botón *Start*.

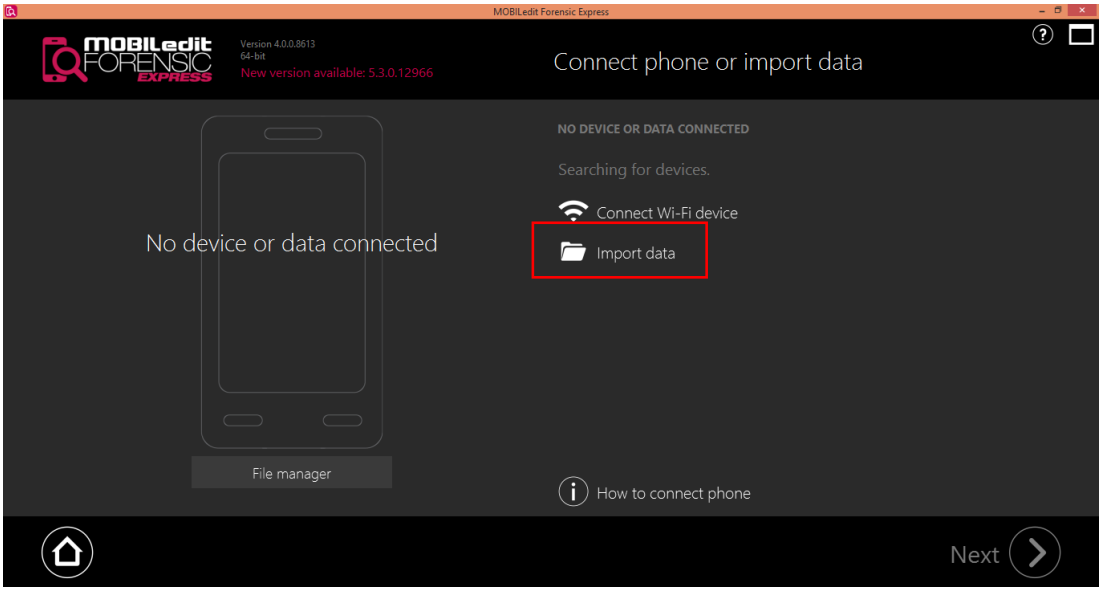


Figura C.35: Importación la imagen forense.

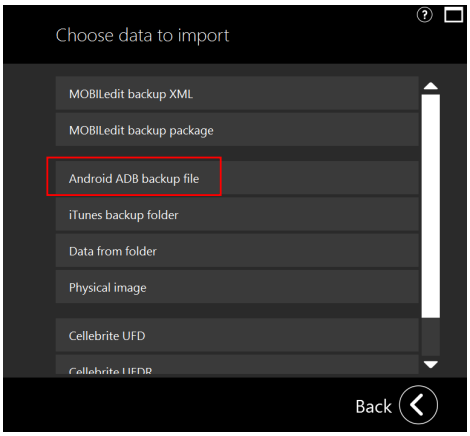


Figura C.36: Se escoge el tipo de imagen que previamente se obtuvo con la misma aplicación.

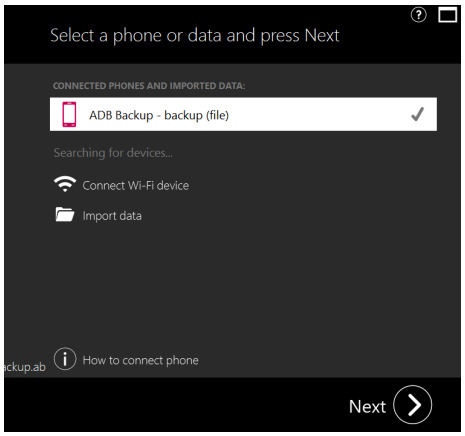


Figura C.37: Se inicia la exportación de los archivos.

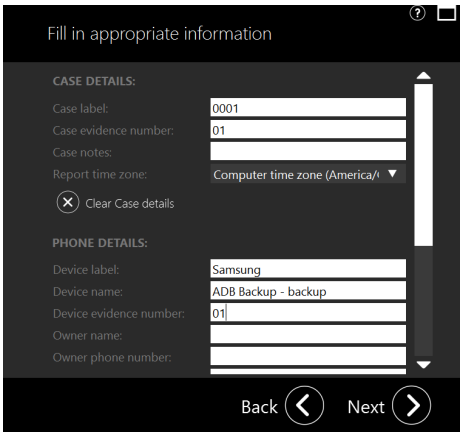


Figura C.38: Ingreso de los datos del caso.

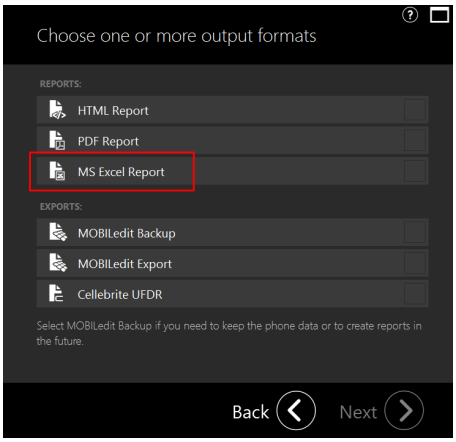


Figura C.39: Selección el formato del reporte.

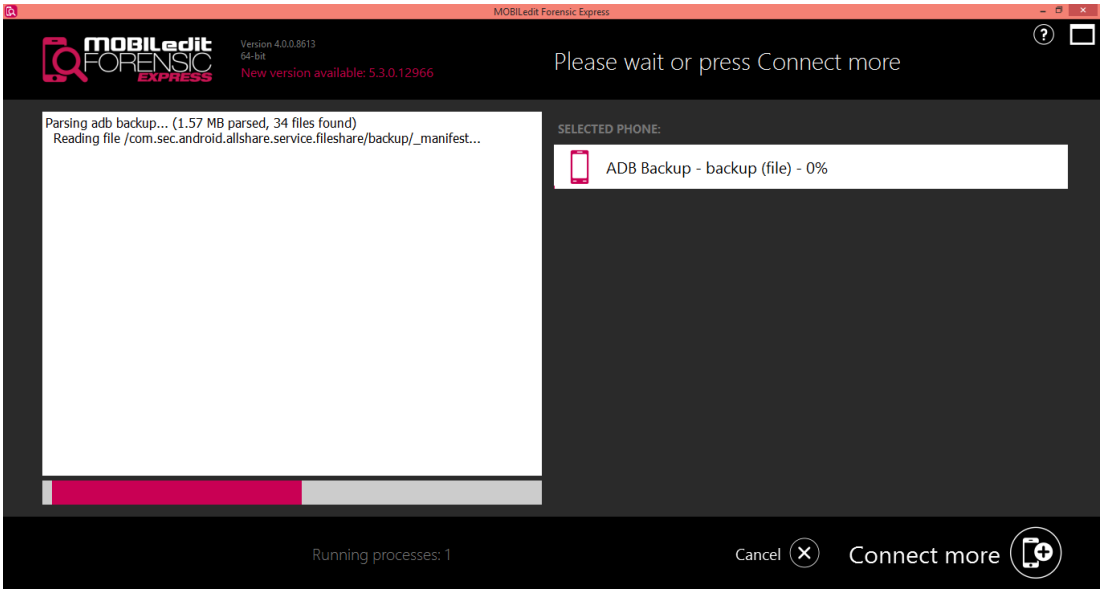


Figura C.40: Iniciación la exportación del archivo.

- Mediante la herramienta Kali Linux se obtiene los reportes de Autopsy, binwalk, bulk_extractor, Chkrootkit, foremost, galleta y volatility.

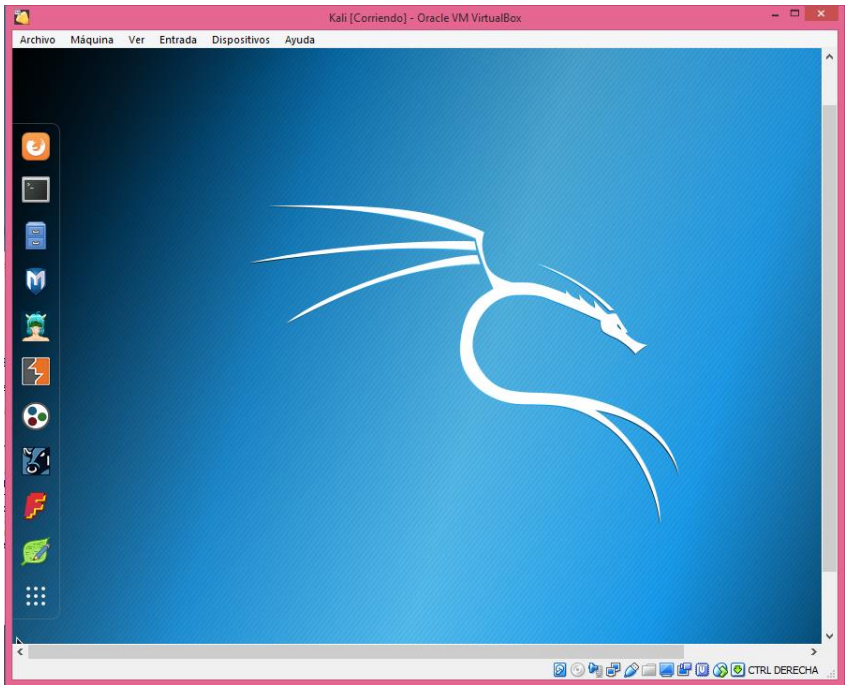


Figura C.41: Presentación de Kali Linux virtualizado en Windows.

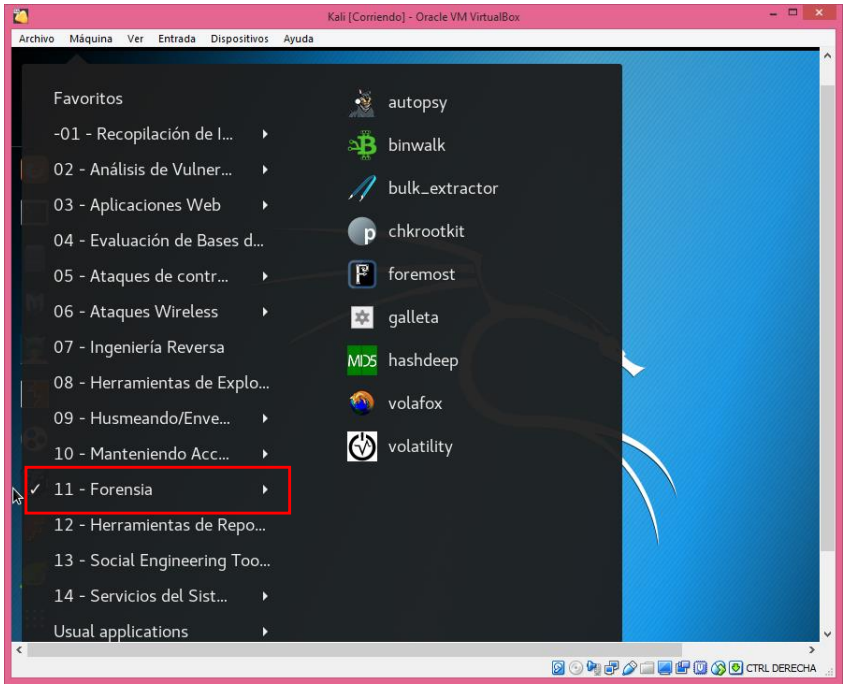


Figura C.42: Selección de la barra aplicaciones para escoger el tipo de herramienta.

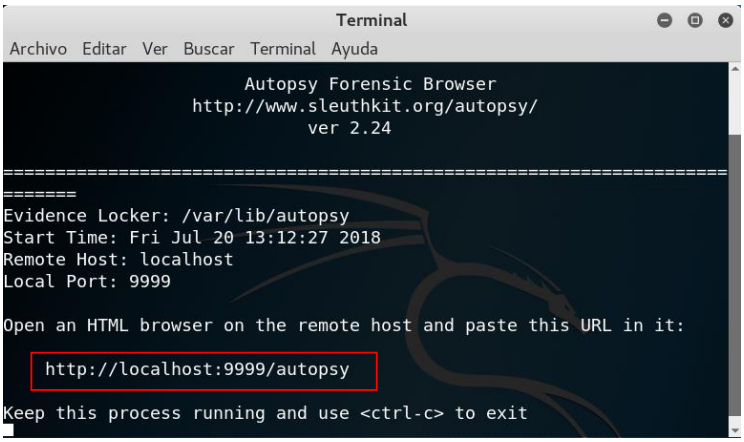


Figura C.43: Terminal ejecutándose Autopsy Forensic Broser.

Figura C.44: Ingreso la dirección en el navegador, se presenta la interfaz de Autopsy.

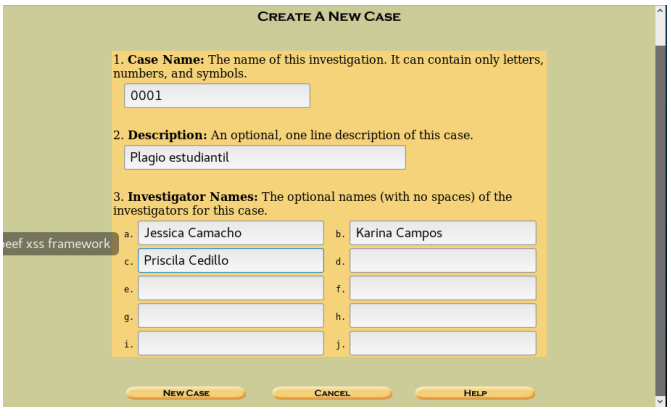


Figura C.45: Se ingresa los datos del caso.

Figura C.46: Se cargar imagen forense y opcional ingresar *host*.

Se ingresa el siguiente comando para la extracción de los archivos donde: *-e* extrae los archivos, *-M* escanea los archivos recursivamente mientras los extrae y *-r* es usado para eliminar cualquier archivo que no se pudo extraer o de tamaño cero.

```
binwalk -Mre imagen
```

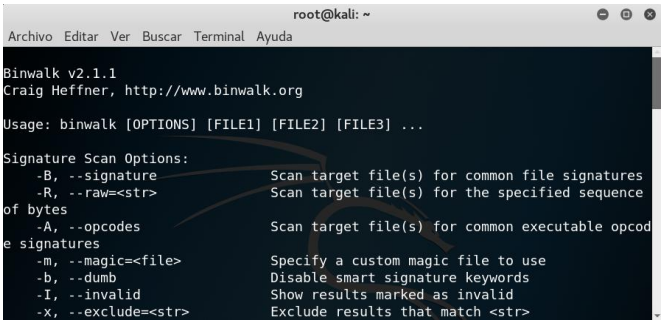


Figura C.47: Terminal ejecutándose Binwalk.

En la consola donde se está corriendo bulk_extractor se ingresa la siguiente línea:

```
bulk_extractor -o reportebulk imagen
```

En la cual *-o* especifica el directorio de salida. Sino existe bulk_extractor crea este directorio.

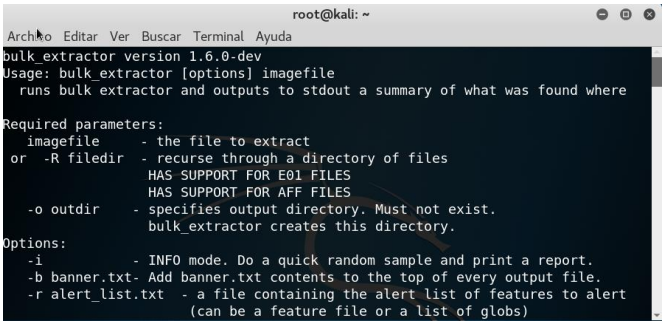


Figura C.48: Terminal ejecutándose bulk_extractor.

Para ésta herramienta es necesario permisos de super usuario, por lo que se debe ejecutar con *sudo*.

```
sudo chkrootkit -q
```

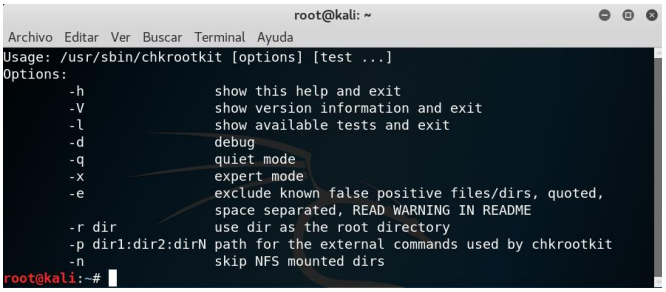


Figura C.49: Terminal ejecutándose chkrootkit.

Mientras que, volatility es otra de las herramientas sencillas de usar y solo se ingresa la siguiente linea de comando:

```
sudo volatility -f imagen imageinfo
```

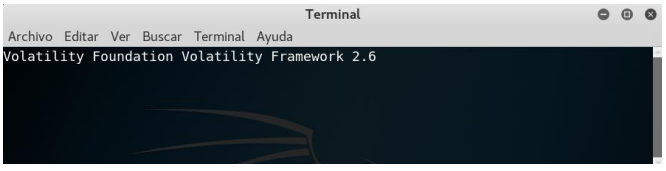


Figura C.50: Terminal ejecutándose Volatility.

Se ejecuta el siguiente comando donde: *all* recuperar todos los archivo, *-i* la dirección donde se va a buscar, *-o* donde se va a guardar.

```
sudo foremost all -i /root/Desktop/imagen -o Desktop/foremost/recuperadoF
```

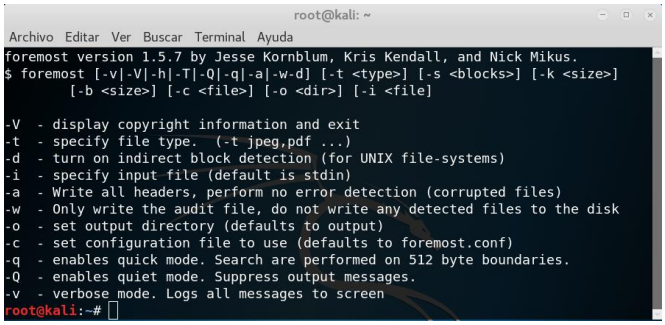


Figura C.51: Terminal ejecutándose foremost.

b. Actividades del usuario

Gracias a las herramientas del punto a se obtuvo los reportes como se observa en las Figuras C.52 y C.53. El paquete de herramientas forenses en Windows arrojó 20 reportes en formato .xls, mientras que, en Linux fueron 6 archivos en formato .tex.

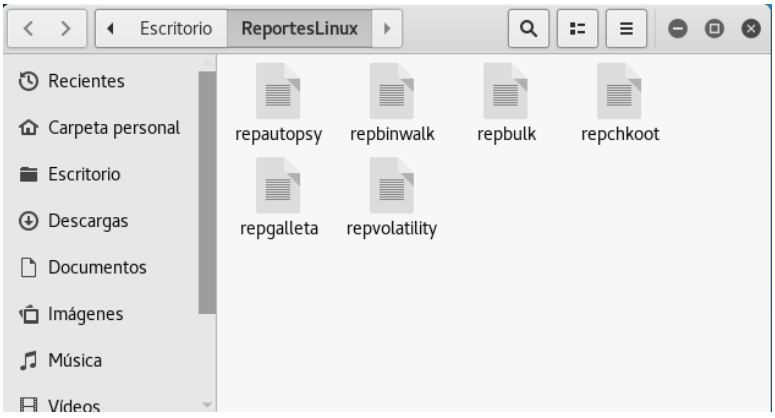


Figura C.52: Terminal ejecutándose Volatility.

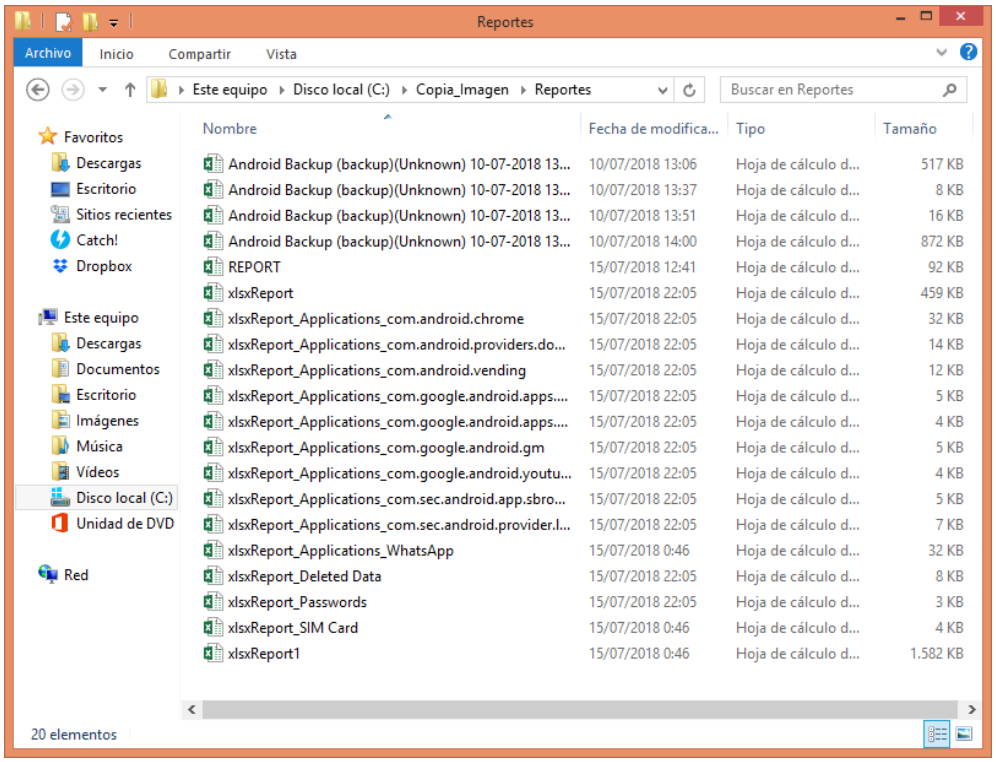


Figura C.53: Terminal ejecutándose Volatility.

Una vez obtenido todos los reportes se procese a guardarlos en un sola carpeta. El primer paso para utilizar la herramienta RegistroActividades es ingresar al terminal y colocar la siguiente linea:

```
python RegistroActividades.py
```

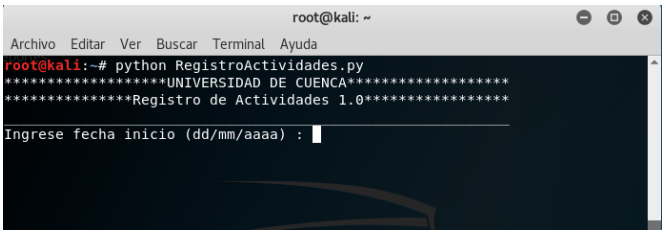


Figura C.54: Terminal ejecutándose RegistroActividades.

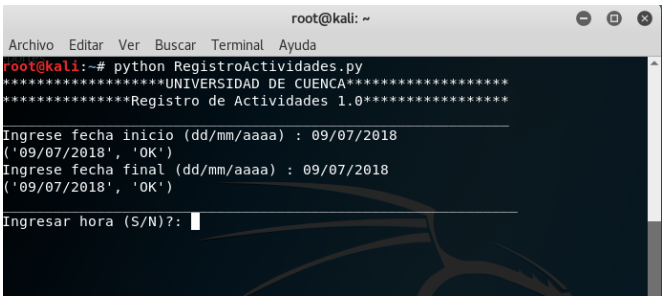


Figura C.55: Se ingresa fecha de inicio y fin.

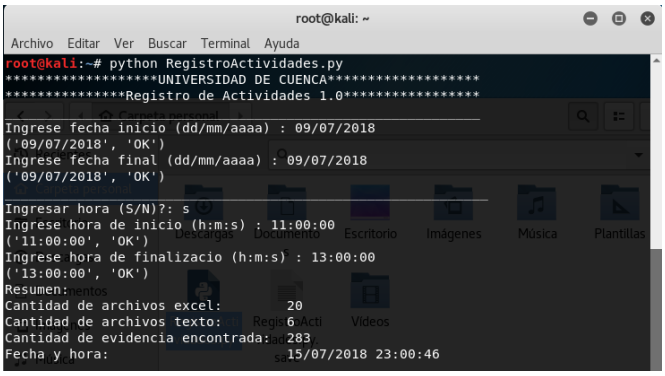


Figura C.56: Se ingresa hora de inicio y fin.

El reporte final se guarda en el escritorio, es un archivo texto el cual contiene 283 actividades durante el periodo que se ingresó. Al analizar y revisar el reporte se llega a la conclusión que 25 actividades son las que tiene relevancia para ésta investigación, por consecuencia se extraen éstas mediante la opción de filtro del mismo programas. Para ver con más detalles todo el registro ver Apéndice B.

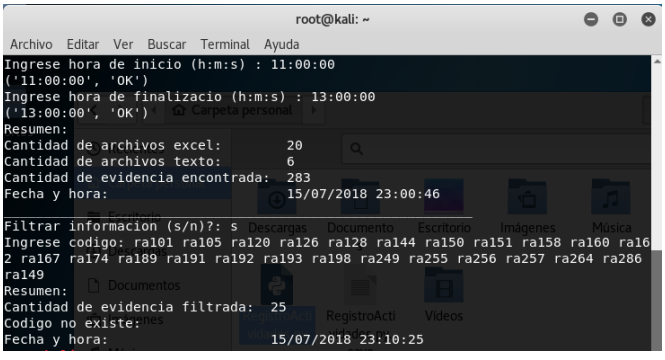


Figura C.57: Ingreso del filtro mediante códigos.

c. Análisis de las actividades relevante para el caso

Se extrae imágenes forense con 3 diferentes herramientas (Andriller, MOBILedit y Oxygen Forensic Analyst) y de cada una se obtuvo diferente información del dispositivo. Posteriormente, se extrajo los datos necesarios para la investigación con los 6 *software* escogidos para este trabajo. Finalmente, con la herramienta de registro de actividades se procedió a filtrar la información para obtener las actividades del día 9 de julio de 2018. Al analizar el registro se obtuvo los siguientes datos más relevantes realizados por el estudiante en el horario de examen de 11h00 a 13h00.

C.5.4. Resultados

Historial de navegación web

El primer acceso que el estudiante desarrolló fue a las 11:40:34, donde se evidencia el ingreso a la aplicación de Google Chrome en la cual realizó la búsqueda "de que es PIM" que es un término utilizado en dicha asignatura. También realizó la búsqueda de términos como: *planificar las repuestas a los riesgos*, *interacción entre grupos de procesos en un proyecto*, *identificación de Riegos*. Todos los términos están estrechamente relacionados con la asignatura de Organización y evaluación de proyectos.

Por otra parte, se puede observar que el estudiante trato de conectarse varias veces a la misma página por tal motivo hay varias etiquetas que presentan la descripción de no existe o en otro caso no se pudo acceder a la página o se abortó el intento.

Todos estas acciones se desenvolvieron en el lapso de 11:40:34 a 12:12:03 el cual concuerda con el horario de examen. En conclusión son 11 actividades en esta sección, a continuación se presenta un resumen que demuestra las búsquedas que el usuario del dispositivo móvil realizó en ese periodo de tiempo:

Etiqueta: que es pim - Buscar con Google
Fecha y hora: 09/07/2018 11:40:34
Eliminado: falso
Número de visita: 1
URL: `https://www.google.com.ec/search?q=que+es+pim&oq=que+es+pim&aqs=chrome..69i57.5378j0j4&client=ms-android-samsung&sourceid=chrome-mobile&ie=UTF-8`

Etiqueta: No existe
Fecha y hora: 2018-07-09 11:43:19
Eliminado: falso

Número de visita: 1 URL: https://www.google.com.ec/amp/s/www.gladysgbegnedji.com/planificar-la-respuesta-a-los-riesgos-2/amp/

Etiqueta: planificar las resouestas a.los riesgos - Buscar con Google
Fecha y hora: 2018-07-09 11:43:52
Eliminado: falso
Número de visita: 2
URL: https://www.google.com.ec/search?q=planificar+las+resouestas+a.los+riesgos&oq=planificar+las+resouestas+a.los+riesgos&aqs=chrome..69i57j0l3.23500j0j9&client=ms-android-samsung&sourceid=chrome-mobile&ie=UTF-8

Etiqueta: 3.- La interacción entre los procesos de la Dirección de Proyectos según La guía del PMBOK® 26-03-2012 – 1ra Parte / La Guía del PMBOK® / Capitulo 3 | formulaproyectosurbanospmipe
Fecha y hora: 2018-07-09 11:47:49
Eliminado: falso
Número de visita: 1
URL: https://formulaproyectosurbanospmipe.wordpress.com/2012/04/25/3-la-interaccion-entre-los-procesos-de-la-direccion-de-proyectos-segun-la-guia-del-pmbok-26-03-2012-1ra-parte-la-guia-del-pmbok-capitulo-3/

Etiqueta: No existe
Fecha y hora: 2018-07-09 11:51:29
Eliminado: falso
Número de visitas: 1
URL: https://formulaproyectosurbanospmipe.files.wordpress.com/2012/04/b3.jpg

Etiqueta: No existe
Fecha y hora: 2018-07-09 11:51:34
Eliminado: falso
Número de visitas: 2
URL: https://www.google.com.ec/search?q=interaccion+entre+los+grupos+de+procesos+en+un+proyecto&client=ms-android-samsung&source=lnms&tbm=isch&sa=X&ved=0ahUKEwi-3rWJx6HcAhWBrFkKHZ4SBZwQ_AUICCgB&biw=320&bih=452#imgrc=sUZ-4sxtkAKSyM%3A

Etiqueta: interaccion entre los grupos de procesos en un proyecto - Buscar con Google
Fecha y hora: 2018-07-09 11:51:37
Eliminado: falso
Número de visitas: 2
URL: https://www.google.com.ec/search?q=interaccion+entre+los+grupos+de+procesos+en+un+proyecto&client=ms-android-samsung&source=lnms&tbm=isch&sa=X&ved=0ahUK

Ewi-3rWJx6HcAhWBrFkKHZ4SBZwQ_AUICCgB&biw=320&bih=452

Etiqueta: interaccion entre los grupos de procesos en un proyecto - Buscar con Google
Fecha y hora: 2018-07-09 11:51:42
Eliminado: falso
Número de visitas: 2
URL: https://www.google.com.ec/search?client=ms-android-samsung&q=interaccion+entre+los+grupos+de+procesos+en+un+proyecto&oq=interaccion+entre+los+grupos+de+procesos+en+un+proyecto&aqs=mobile-gws-lite.....3

Etiqueta: Identificación de riesgos en proyectos. Qué es y técnicas para hacerla.
Fecha y hora: 2018-07-09 11:57:12
Eliminado: falso
Número de visitas: 1
URL: https://www.recursosenprojectmanagement.com/identificacion-de-riesgos/

Etiqueta: No existe
Fecha y hora: 2018-07-09 12:02:02
Eliminado: falso
Número de visitas: 1
URL: https://www.google.com.ec/search?q=identificacion+de+riesgos&oq=identificacion+de+riesgos&aqs=chrome..69i57j0l3.9070j0j9&client=ms-android-samsung&sourceid=chrome-mobile&ie=UTF-8#imgrc=9-SwZ7VVUuKhNM%3A

Etiqueta: No existe
Fecha y hora: 2018-07-09 12:03:19
Eliminado: falso
Número de visitas: 1
URL: https://www.google.com.ec/search?q=identificacion+de+riesgos&client=ms-android-samsung&source=lnms&tbm=isch&sa=X&ved=0ahUKEwis-cLxyKHcAhXRjVkKHXwzDWUQ_AUICCgB&biw=320&bih=452#imgrc=9-SwZ7VVUuKhNM%3A

Etiqueta: identificacion de riesgos - Buscar con Google
Fecha y hora: 2018-07-09 12:03:47
Eliminado: falso
Número de visitas: 2
URL: https://www.google.com.ec/search?q=identificacion+de+riesgos&client=ms-android-samsung&source=lnms&tbm=isch&sa=X&ved=0ahUKEwis-cLxyKHcAhXRjVkKHXwzDWUQ_AUICCgB&biw=320&bih=452

Etiqueta: identificacion de riesgos - Buscar con Google

Fecha y hora: 2018-07-09 12:03:53
Eliminado: falso
Número de visitas: 1
URL: https://www.google.com.ec/search?q=identificacion+de+riesgos&oq=identificacion+de+riesgos&aqs=chrome..69i57j0l3.9070j0j9&client=ms-android-samsung&sourceid=chrome-mobile&ie=UTF-8

Etiqueta: organizacion de proyectos - Buscar con Google
Fecha y hora: 2018-07-09 12:12:04
Eliminado: falso
Número de visitas: 1
URL: https://www.google.com.ec/search?q=organizacion+de+proyectos&oq=organizacion+de+proyectos&aqs=chrome..69i57.7650j0j1&client=ms-android-samsung&sourceid=chrome-mobile&ie=UTF-8

Etiqueta: organizacion de proyectos - Buscar con Google
Fecha y hora: 2018-07-09 12:12:12
Eliminado: falso
Número de visitas: 1
URL: https://www.google.com.ec/search?q=organizacion+de+proyectos&client=ms-android-samsung&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjA0oSezKHcAhVow1kKHXVeA0cQ_AUICCgB&biw=320&bih=452

Etiqueta: No existe
Fecha y hora: 2018-07-09 12:12:22
Eliminado:falso
Número de visitas:
URL: https://www.google.com.ec/search?q=organizacion+de+proyectos&client=ms-android-samsung&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjA0oSezKHcAhVow1kKHXVeA0cQ_AUICCgB&biw=320&bih=452#imgrc=BwgJIffsTOe0IM%3A

Etiqueta: No existe
Fecha y hora: 2018-07-09 12:12:29
Eliminado: falso
Número de visitas: 2
URL: https://www.google.com.ec/search?q=organizacion+de+proyectos&client=ms-android-samsung&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjA0oSezKHcAhVow1kKHXVeA0cQ_AUICCgB&biw=320&bih=452#imgrc=aMiFeSxm-Vo5jM%3A

Etiqueta: No existe
Fecha y hora: 2018-07-09 12:12:30

Eliminado: falso
Número de visitas: 3
URL: https://www.google.com.ec/search?q=organizacion+de+proyectos&client=ms-android-samsung&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjA0oSezKHcAhVow1kKHXVeA0cQ_AUICCgB&biw=320&bih=452#imgrc=Q8Wpv7HWxASeqM%3A

Cookies

Analizando el archivo de cookies arrojó que el estudiante accedió al navegador como ya se mencionó en la parte a de resultados. Se ingresó en el navegador en el lapso de 11:40:52 a 12:12:10 como se observa en la Tabla C.7, en el cual se corrobora que buscaba temas referente a la asignatura como: fórmula proyectos urbanos pmi y recursos en proyect management.

Tabla C.7: Evidencia cookies

Etiqueta	Eliminado	Fecha	Hora	Sitio
NID	false	2018-07-09	11:40:52	.google.com.ec
eucookielaw	false	2018-07-09	11:49:45	formulaproyectosurbanospmipe.wordpress.com
personalized -ads-consent	false	2018-07-09	11:49:45	formulaproyectosurbanospmipe.wordpress.com
_ga	false	2018-07-09	11:56:38	.www.recursosenprojectmanagement.com
_gid	false	2018-07-09	11:56:38	.www.recursosenprojectmanagement.com
1P_JAR	false	2018-07-09	12:01:06	.google.com.ec
GAPS	false	2018-07-09	12:11:36	accounts.google.com
SIDCC	false	2018-07-09	12:12:10	.google.com

Imágenes

En cuanto a las imágenes, durante el examen, esto es en entre las 10:55:44 y 11:00:20 realizó cuatro capturas de pantalla de un computador como se observa en la Tabla C.8. Al recuperar dichas imágenes se observa que corresponden a temas referentes a la asignatura como: escala de impacto, escala de probabilidad, riesgos que afectan entre otros y que el estudiante pudo utilizar en el examen como ayuda, se puede apreciar en las Figuras C.58 y C.59 las fotografías recuperadas.

Tabla C.8: Evidencia con imágenes

Nombre imagen	Fecha	Eliminada	Tamaño
20180709_115544.jpg	2018-07-09 11:55:44		2560x1536
20180709_115549.jpg	2018-07-09 11:55:59		2560x1536
20180709_115626.jpg	2018-07-09 11:56:23		2560x1536
20180709_120020.jpg	2018-07-09 12:00:20		2560x1536

Figura C.58: Imágenes recuperadas: escala de impacto.

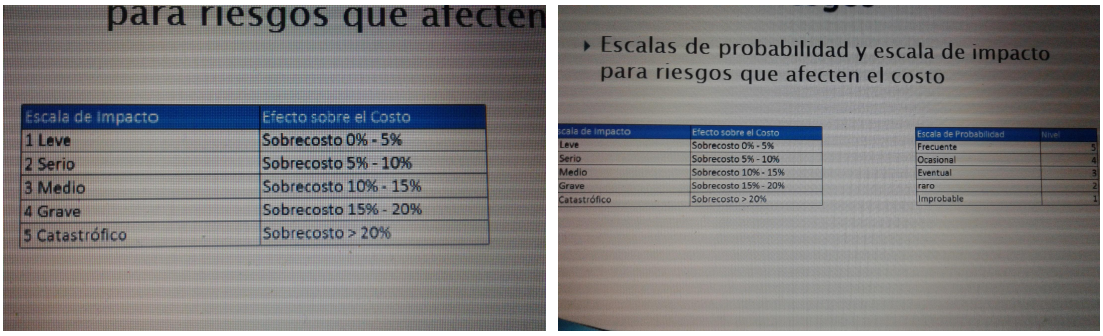


Figura C.59: Imágenes recuperadas: cuadros comparativos riesgos.

Descargas

En esta sección se obtuvo dos actividades realizadas: descarga de navegación y tránsito como también otra descarga de un pdf como se observa en la Tabla C.9. La primera descarga no es relevante para la asignatura pero confirma que si estuvo manipulando el teléfono. Mientras que, en la segunda descarga se obtuvo un pdf con el tema de identificación de los riesgos que se relaciona con la asignatura.

Tabla C.9: Evidencia descargas

Etiqueta	Fecha	Hora	Sitio/URL
Maps: Navegación y tránsito	2018-07-09	12:16:36	https://play.googleapis.com/download/by-token
3Identificacionde losRiesgos_es.pdf	2018-07-09	12:04:20	non-dwnldmngr-download-dont-retry2download

Aplicaciones: WhatsApp

En la parte de aplicaciones solo se obtuvo información relevante para el caso con WhatsApp. Se obtuvo que el estudiante envió un mensaje de voz a las 11:26:44 como se observa en la Tabla C.10 se adjunta la dirección donde se puede recuperar el mensaje.

Tabla C.10: Evidencia aplicaciones

Etiqueta	Fecha	Hora	Ruta	Nombre del archivo
/Stored Audio	2018-07-09	11:26:44	phone/applications0/ com.whatsapp /live_specific/Media /WhatsApp	AUD-20180709-WA0000.opus

Aplicaciones del Sistema

Finalmente, en la Tabla C.11 se muestra todas las actividades que el sistema del dispositivo móvil guarda por defecto. Este comprueba que si hubo actividad en este periodo.

Observaciones

- En primer lugar para determinar si los datos adquiridos mediante las herramientas se relacionaban con la asignatura se tuvo que pedir información al docente sobre el o los temas que trataba el examen.

Etiqueta	Ruta	Fecha	Hora
3Identificaciondelos Riesgos_es.pdf	phone/applications0/0/backup/Download /3IdentificaciondelosRiesgos_es.pdf	2018-07-09	12:04:20
zzzKeyboard_070a _010A_480x296.xml	phone/applications0/0/backup/data /zzzKeyboard_070a_010A_480x296.xml	2018-07-09	12:08:54
_manifest	phone/applications0/android/backup /_manifest	2018-07-09	12:08:52
_manifest	phone/applications0/com.android.browser. provider/backup/_manifest	2018-07-09	12:28:49
_manifest	phone/applications0/com.android.calendar /backup/_manifest	2018-07-09	12:27:33
29abb1c1d5088b28_0	phone/applications0/com.android.chrome /backup/r/app_chrome/Default/GPUCache /2042621ecce1d831_0	2018-07-09	11:49:43
2e11213a2fcadbeb_0	phone/applications0/com.android.chrome /backup/r/app_chrome/Default/GPUCache /29abb1c1d5088b28_0	2018-07-09	11:41:18
354dc64e7e1dbc96_0	phone/applications0/com.android.chrome /backup/r/app_chrome/Default/GPUCache /2e11213a2fcadbeb_0	2018-07-09	11:08:23
354dc64e7e1dbc96_0	phone/applications0/com.android.chrome /backup/r/app_chrome/Default/GPUCache /354dc64e7e1dbc96_0	2018-07-09	11:49:43
002465.log	phone/applications0/com.android.chrome /backup/r/app_chrome/Default/Local Storage /leveldb/002465.log	2018-07-09	11:57:36

Tabla C.11: Evidencia aplicaciones del sistema

Etiqueta	Ruta	Fecha	Hora
_manifest	phone/applications0/com.android.chrome /backup/_manifest	2018-07-09	12:29:38
BrowserMetrics-spare.pma	phone/applications0/com.android.chrome /backup/r/app_chrome/BrowserMetrics-spare.pma	2018-07-09	12:29:38
Local State	phone/applications0/com.android.chrome /backup/r/app_chrome/Local Satate	2018-07-09	12:29:38
Cookies	phone/applications0/com.android.chrome /backup/r/app_chrome/Default/Cookies	2018-07-09	12:29:38
Favicons	phone/applications0/com.android.chrome /backup/r/app_chrome/Default/Cookies-journal	2018-07-09	12:29:38
Favicons-journal	phone/applications0/com.android.chrome /backup/r/app_chrome/Default/Favicons	2018-07-09	12:29:38
History	phone/applications0/com.android.chrome /backup/r/app_chrome/Default/Favicons-journal	2018-07-09	12:29:38
History-journal	phone/applications0/com.android.chrome /backup/r/app_chrome/Default/History	2018-07-09	12:29:38
Login Data	phone/applications0/com.android.chrome /backup/r/app_chrome/Default/History-journal	2018-07-09	12:29:38
Login Data-journal	phone/applications0/com.android.chrome /backup/r/app_chrome/Default/Login Data	2018-07-09	12:29:38
Network Persistent State	phone/applications0/com.android.chrome /backup/r/app_chrome/Default/Network Persistent State	2018-07-09	12:29:38
Preferences	phone/applications0/com.android.chrome /backup/r/app_chrome/Default/Preferences	2018-07-09	12:29:38
QuotaManager-journal	phone/applications0/com.android.chrome /backup/r/app_chrome/Default/Network Persistente State	2018-07-09	12:29:38
TransportSecurity	phone/applications0/com.android.chrome /backup/r/app_chrome/Default/ TransportSecurity	2018-07-09	12:29:38
Web Data	phone/applications0/com.android.chrome /backup/r/app_chrome/Default/QuotaManager	2018-07-09	12:29:38
in_progress_ download_ metadata_store	phone/applications0/com.android.chrome /backup/r/app_chrome/Default/ TransportSecurity	2018-07-09	12:29:38
000226.log	phone/applications0/com.android.chrome /backup/r/app_chrome/Default/Download	2018-07-09	12:29:38

Etiqueta	Ruta	Fecha	Hora
CURRENT	phone/applications0/com.android.chrome /backup/r/app_chrome/Default/Download Service/EntryDB/CURRENT	2018-07-09	12:12:01
LOG	phone/applications0/com.android.chrome /backup/r/app_chrome/Default/Download Service/EntryDB/LOG.old	2018-07-09	12:12:01
LOG.old	phone/applications0/com.android.chrome /backup/r/app_chrome/Default/ Download Service/EntryDB/LOG.old	2018-07-09	12:00:53
MANIFEST-000225	phone/applications0/com.android.chrome /backup/r/app_chrome/Default/ Download Service/EntryDB/MANIFEST-000225	2018-07-09	12:12:01
000003.log	phone/applications0/com.android.chrome /backup/r/app_chrome/Default /Feature Engagement Tracker/AvailabilityDB/LOG	2018-07-09	12:12:03
LOG	phone/applications0/com.android.chrome /backup/r/app_chrome/Default /Feature Engadement Tracker/AvaibilityDB/LOG	2018-07-09	12:12:02
LOG.old	phone/applications0/com.android.chrome /backup/r/app_chrome/Default /Feature Engadement Tracker/AvaibilityDB/LOG	2018-07-09	12:00:54
000003.log	phone/applications0/com.android.chrome /backup/r/app_chrome/Default Engadement Tracker/AvabilityDB/LOG	2018-07-09	12:04:20
LOG	phone/applications0/com.android.chrome /backup/r/app_chrome/Default /Feature Engagement Tracker/EventDB/LOG	2018-07-09	12:12:02
LOG.old	phone/applications0/com.android.chrome /backup/r/app_chrome/Default Engagement Tracker/EventDB/LOG	2018-07-09	12:00:54
LOG	phone/applications0/com.android.chrome /backup/r/app_chrome/Default /File System/Origins/LOG	2018-07-09	11:39:52
06f6435a243693a0_0	phone/applications0/com.android.chrome /backup/r/app_chrome/Default/GPUCache /06f6435a243693a0_0	2018-07-09	11:49:45
192b63747196de2e_0	phone/applications0/com.android.chrome /backup/r/app_chrome/Default/GPUCache /192b63747196de2e_0	2018-07-09	11:49:33

C.6. DECLARACIÓN JURAMENTADA

Yo, Jessica Camacho Cajamarca, de nacionalidad ecuatoriana, de estado civil soltera, mayor de edad, estudiante de la carrera de Ingeniería Electrónica y Telecomunicaciones, domiciliada en la ciudad de Azogues y legalmente capaz, declaro bajo juramento que el informe presentado es independiente y corresponde a mi real convicción profesional, así como también declaro que toda la información que he presentado es verdadera.

C.7. FIRMA Y RÚBRICA

Srta. Jessica Camacho Cajamarca
Estudiante de la carrera de Ingeniería Electrónica y Telecomunicaciones
CI: 0301836466

Apéndice D

Producción Científica

El artículo “A Systematic Literature Review in Cyber Forensics: Current Trends from the Client Perspective” fue aceptado en la conferencia IEEE ETCM (Ecuador Technical Chapters Meeting) 2018 en su tercera edición, posteriormente será incluido en la biblioteca digital IEEE Xplore. Mientras que, el artículo “Forensics Analysis on Mobile Devices: A Systematic Mapping Study” fue aceptado en la conferencia TIC.EC (Information and Communication Technologies of Ecuador) 2018 en su sexta edición y posteriormente publicado en Springer. Finalmente, se desarrolló el artículo “A Forensics Activity Logger to Extract User Activity from Mobile Devices”.

Forensics Analysis on Mobile Devices: A Systematic Mapping Study

Abstract. Nowadays, mobile devices have evolved vertiginously due to their massive adoption by users, who have several devices with different purposes. These devices contain greater capacity / functionality to manage information, with the embedded characteristics they become an important digital evidence container. In recent years, considerable research has been conducted on various digital electronic evidence, acquisition schemes and methods of extracting evidence from mobile devices. In this paper, a systematic mapping of the Forensics Analysis on Mobile Device is presented, this research has been conducted following the guidelines of Kitchenham's methodology. The aim of this study is to provide a background of relevant activities that are considered by investigators to handle with potentially digital evidence from mobile devices. A total of 36 primary studies were selected and categorized to extract information regarding the aforementioned classification. The results presented in this contribution provide a detailed study about current analysis in research forensics field by using mobile devices.

Keywords: Forensics; Digital Evidence; Devices.

1 Introduction

Nowadays, mobile devices are being used massively, becoming one of the best inventions that have existed, mainly because of their functionality, contents, and versatility. Smartphones are mini computers that provide the functionality of conventional telephones, wireless Internet access, and, recently, many booming applications. They also provide sources of information in real time, exchange of data and information on a daily basis. Besides, they represent an interesting source of proof for crime research due to the content that can be found stored on one of those devices (e.g., bank transactions, social interaction). Fraudsters and other cyber criminals can use different services provided by platforms with false identities, in order to hide their malicious intentions behind profiles that seem to be reliable.

The digital forensic analysis has been defined as the use of scientifically derived and proven methods for the preservation, collection, validation, identification, analysis, interpretation and presentation of digital evidence [S09]. The challenge of preserving and managing the evidence existing in mobile devices has motivated the creation of methods and solutions to manage the evidence in a properly way.

As far as it is known, no evidence-based studies (e.g., systematic mapping studies, systematic literature reviews) have been recently reported about the considerations with which forensic tools perform treatment of electronic digital evidence into mobile devices. A systematic mapping study is a way to categorize and summarize the existing information around a research question in an unbiased manner [6]. Therefore, a

A Systematic Literature Review in Cyber Forensics: Current Trends from the Client Perspective

***Abstract*— Nowadays, with the demand of web applications there is also an increase in the number of problems and crimes that demand an investigation that requires digital forensics techniques in order to manage web evidence. Although there are several studies that address cyber forensics, they are mainly oriented to manage evidence at server side, as far as we know, no systematic literature reviews have been reported on how cyber forensics is addressed at clients' side; considering the internationals standards. Thus, this paper reports a literature review about how cyber forensics is addressed at clients' side related to techniques of identification, collection, analysis, preservation and report of digital evidence. Also, a review of how standards are being used in cyber forensics focused on the client side. The aim of this study is to provide a background of relevant activities that are considered by investigators to handle with potentially digital evidence from web environments, considering what internationals standards are solving for this purpose. Thus, a total of 37 studies have been selected and analyzed in this study. Moreover, this study provides important insights about the need to create methodologies aligned with formal standards that support the management of the evidence in an appropriate way.**

Keywords*— *digital evidence, cyber forensics, client side, systematic review, standards

I. Introduction

Currently, web applications have been adopted in the most of transactional systems of organizations. Also, there are applications deployed on web environments for different purposes (e.g., social networks, email, cloud storage). With the mass use of online applications, there is also an increase in the number of crimes, cyber-attacks, and punishable by law activities [1]. In general, people use web browsers or desktop applications that request pages and resources to a server; therefore, it is important to manage digital evidence left in client's computers by using suitable forensics guidelines [2].

Moreover, with the emergence of new web technologies and cloud computing with their service models (i.e., Infrastructure as a Service, Platform as a Service and Software as a Service) [3] the importance of digital evidence has increased substantially [4]. Also, there are studies that consider the current increase in the number of applications deployed on the cloud, several authors address their studies in a similar way to both web and SaaS (Software as a Service) applications at client's side [5], [6], because in both cases forensics investigators do not have access to the server.

Then, a literature review is a way to identify, evaluate, and interpret all available research relevant to a particular topic area, or phenomenon of interest [7]. There are studies that provide systematic reviews or mappings about cyber forensics and the managing of digital evidence [8]–[10]. Thus, Guo et al., [8] provide concepts, principles, and a process for performing a forensic investigation; however, they do not cover cyber forensics and it specific considerations at client's side. In addition, Hatole y Bawiskar [9] present a literature review about email forensics, they also present techniques and tools; however, this study addresses a forensics process only for emails. Finally, Kaur et al. [10] propose a literature review on cyber forensics and its analysis tools; however, they are focused on general aspects without taking into account the client perspective and the classification of the evidence that investigators can find.

Consequently, this paper presents a secondary study about cyber forensics with guidelines that support the forensics management from web environments focused on the client-side. Also, it analyses the standards that can be useful for forensics investigations, and there are: (i) ISO/IEC 27037, which reviews guidelines for identification, collection, acquisition, and preservation of the digital evidence [11]; (ii) ISO/IEC 27042 that provides guidelines for the analysis and interpretation of digital evidence [12]; (iii) ISO/IEC 27041 that provides guidance on assuring suitability and adequacy of incident investigative method [13]; (iv) ISO/IEC 27017, which is a code of practice for information security controls based on ISO/IEC 27002 but can be used specifically for cloud services [14]; and finally, (v) ISO/IEC 27050 that provides requirements and guidance on activities in electronic discovery [15]. The result of this systematic review is an overview of current research studies related to cyber forensics in order to manage digital evidence from web environments at the client side.

Finally, this paper is structured as follows: Section 2 presents an overview of the state of the research related to web forensics at client's side. In Section 3 it is described the research method that is used to identify the relevant literature related to this contribution. Section 4 presents the results of the research method and describes the relevant approaches according to the mentioned classification. Section 5 presents a discussion of the results obtained by the followed methodology according to the literature. Finally, the conclusions are presented in Section 6.

II. Related Work

There are some secondary studies related to guidelines to manage digital evidence from web environments [8]–[10], [16]–[18]. Therefore, Guo et al. [8] present some definitions and principles related to computer forensics and digital evidence; however, the authors study the digital evidence in a general way, without specifically considering obtaining evidence on the client's side. On the other hand, Garfinkel [17] presents a literature review where the author addresses the problems of current forensics processes and challenges in the near future; however, the author does not cover digital evidence from web environments. Simou et al. [16] address a review of cloud forensics; the authors are focused on available technical solutions presented in primary studies that have applicability on cloud computing specifically the SaaS service model; and provide general guidelines to be considered respected to artifacts in that service model.

A Forensics Activity Logger to Extract User Activity from Mobile Devices

***Abstract*—Mobile devices have become one of the most powerful and necessary tools in the life of people; therefore, they contain personal information, and constitutes a personal tracker of activities. In this context, mobile devices can provide important information of the activity of a person. Thus, a lot of tools have emerged to provide information about the use of those devices. However, each tool provides isolated information about specific applications and activity. Therefore, this paper proposes a tool that helps investigators to get a complete and merged report and timeline of the activities performed by the device user. In order to illustrate the use of this tool, an example is presented, in which is presented the steps to be followed when using the proposed tool.**

Keywords*—*forensics; tool; register; activity; mobile; smartphone; Android

I. Introduction

Nowadays, mobile devices have become an indispensable tool for people around the world. These devices are used for a wide spread of tasks (e.g., entertainment, education, communication, socialization, research). Therefore, they store information related to those activities. However, they can also constitute an important source of evidence for forensics analysis, which serve as support for judicial cases, helping judges in taking decisions [1].

On the other hand, the forensics analysis use a set of techniques that allow the collection and extraction of information from different devices without altering their original state [2]. For example, it can be recovered deleted files, browsing history, instant messaging information, login data, among others. All this information is known as digital evidence []. However, sometimes that information is not relevant; this situation causes the analysis of impractical information [3]. According to Iorio et al., [4], there are three aspects that should be considered during the forensics analysis: i) avoid contamination of the evidence to prevent misinterpretations; ii) act methodically, that is, all the results of the forensics process must be well documented; and iii) control the chain of custody responding to a diligence and special formality to document. In the forensic investigation, there are also legal aspects that are not always met, these leads to the misuse of applications, fraud, theft, dissemination of copyrighted materials, etc. On the other hand, and in order to obtain digital evidence, the analysis carried out by Taylor et al., [5] indicates that it is necessary to follow all the legal guidelines corresponding to the jurisdiction where the conflict is generated. This, in order to avoid undue exposure of personal information. However, from what has been reviewed in this study, there is no tool in the market, which allows the extraction of a log about the behavior of a user of a mobile device as a timeline.

Also, there are a variety of applications (e.g., Encase, DFF, FTK, Helix, Oxygen, MOBILEdit, UFED) for forensic analysis those tools support the inspection of various elements of mobile devices (e.g., internal memory, applications, messages). Now, the so-called suites take all the previous points and join them in a single analysis creating a powerful and useful tool [6]. Also, it is important to take into account that there are advantages of using open source tools for forensics analysis during the investigation (e. g., no-cost, easy to examine in court, allow the verification) [7]. On the other hand, commercial tools are used since they provide a great variety of alternatives for analysis [7]. In Yadav et al., [8] it is presented a comparison between 6 commercial and open source applications. Those tools perform processes such as: recovering, performing keyword searches, recovering cookies, creating forensic images and locating partitions of the digital devices. Also, Shortall and Azhar [9] present two major tools: UFED by Cellebrite and Oxygen by Oxygen Forensics. UFED looks for physical data on the hard drive in order to recover deleted data. Another software for mobile forensics is Oxygen Forensic Suite. This tool has a lot of options to perform a deep forensics analysis. Then, Tajuddin and Manaf [10] explain some popular forensic tools as: Cellebrite UFED, MOBILedit Forensic, Forensic Toolkit, XRY, Oxygen Forensic Suite, EnCASE Forensic, and Paraben's device seizure. Each one has different capabilities, effectiveness and options to acquire information. On the other hand, each software tool offers similar services, analysis techniques and ways to present retrieved data. In the analyzed studies, and as far as we know, there are not solutions that provide a log of the users' actions in using a mobile device. Thus, this paper presents a tool, which generates reports about the mobile device owners' behavior. Also, this tool has been implemented in Python [11]. This tool moreover collects information from different applications dedicated to the data extraction for forensics analysis from mobile devices that have the Android OS. This information is useful in obtaining a track of the users' activities performed by using the mobile device.

The present work is organized as follows: section 2 presents the related work, section 3 presents building the solution, section 4 says operation of registration activities, section 5 discusses the implementation of tool forensics, section 6 a proof of concept is developed to analyze the digital information generated by a mobile device and describes the results obtained with the tool and finally, the conclusions and future work.

II. Related Work

Forensics analysis for mobile devices have been studied in the recent literature, which is mostly focused on Android and iOS operating systems [12]. On the other hand, the forensics analysis is oriented to the study of specific applications. According to Anglano et al, [13] the analysis of instant messaging (IM) applications on smart devices have been addressed in many published studies. The authors also study the artifacts generated by WhatsApp deployed on devices with